(19)日本国特許庁（ＪＰ）　(12)公表特許公報（Ａ）　(11)特許出願公表番号

特表平10－512074

(43)公表日　平成10年(1998)11月17日

(51)Int.Cl.[6]		識別記号	FI		
Ｇ０６Ｆ	15/00	３３０	Ｇ０６Ｆ	15/00	３３０Ｚ
Ａ６３Ｆ	9/22		Ａ６３Ｆ	9/22	Ａ
Ｇ０６Ｆ	13/00	３５１	Ｇ０６Ｆ	13/00	３５１Ｅ
		３５５			３５５
	17/30		Ｇ０９Ｃ	1/00	６６０Ｃ

審査請求　未請求　予備審査請求　有　（全837頁）　最終頁に続く

(21)出願番号　特願平8－526318
(86)(22)出願日　平成８年(1996)２月13日
(85)翻訳文提出日　平成９年(1997)８月13日
(86)国際出願番号　ＰＣＴ／ＵＳ９６／０２３０３
(87)国際公開番号　ＷＯ９６／２７１５５
(87)国際公開日　平成８年(1996)９月６日
(31)優先権主張番号　０８／３８８，１０７
(32)優先日　1995年２月13日
(33)優先権主張国　米国（ＵＳ）

(71)出願人　インタートラスト　テクノロジーズ　コーポレイション
アメリカ合衆国　カリフォルニア　94086－4708，サニーベール，オークメッド　パークウェイ　460
(72)発明者　ジンター，カール　エル．
アメリカ合衆国　メリーランド　20705，ベルツビル，43アールディー　アベニュー　10404
(72)発明者　シェアー，ビクター　エイチ．
アメリカ合衆国　メリーランド　20814，ベセスダ，バッテリー　レーン　5203
(74)代理人　弁理士　山本　秀策

最終頁に続く

(54)【発明の名称】　安全な取引管理および電子権利保護のためのシステムおよび方法

(57)【要約】
本発明は、安全な取引管理および電子権利保護を有する電子商取引のシステムおよび方法を提供する。本発明に従って用いられるコンピュータなどの電子機器は、承認された様式でのみアクセスおよび使用されることを確実にし、情報の完全性、可用性、および／または秘匿性を維持する助けをする。このような電子機器と共に用いられる安全なサブシステムは、例えば、電子的に格納されたまたは広められた情報の使用を制御および／または計量もしくはモニタするために、処理と制御の安全なチェーンを実施し得る配布された仮想配布環境（VDE）を提供する。このような仮想配布環境は、電子商取引および他の電子取扱または電子的に容易になった取扱において様々な参加者の権利を保護するために使用され得る。安全な配布されたおよび他の動作システム環境およびアーキテクチャは、例えば、各ノードで安全な保護された環境を確立し得る安全な半導体処理配置を使用する。これらの技術は、例えば、「電子ハイウェイ」を利用して用いられ得る終端間電子情報配布能力を支持するために使用され得る。

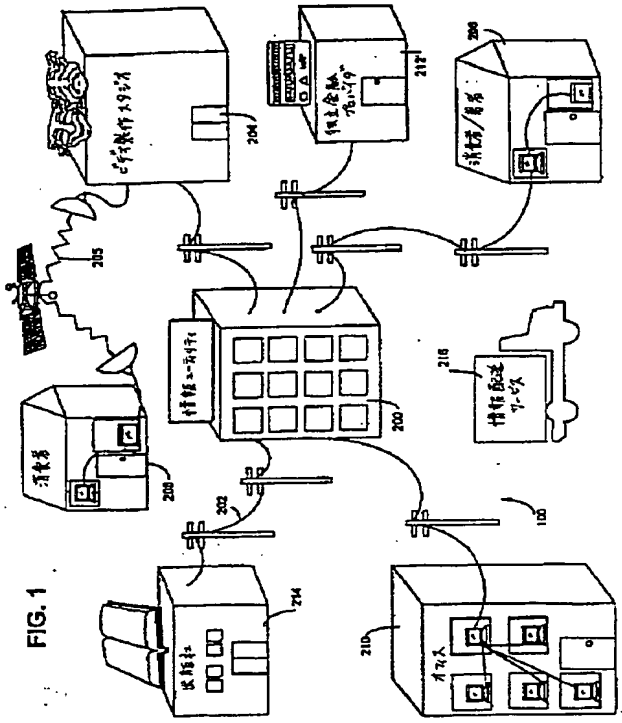


FIG. 1

【特許請求の範囲】

１．安全なコンテンツ配送方法であって、

ａ）１つまたはそれ以上のデジタルコンテナ内にデジタル情報をカプセル化する工程と、

ｂ）該デジタル情報の少なくとも一部を暗号化する工程と、

ｃ）インタラクションを管理するための少なくとも部分的に安全な制御情報と、該暗号化されたデジタル情報および／または該デジタルコンテナとを関連づける工程と、

ｄ）該１つまたはそれ以上のデジタルコンテナの１つまたはそれ以上をデジタル情報ユーザに配送する工程と、

ｅ）該デジタル情報の少なくとも一部の復号化を安全に制御する保護された処理環境を使用する工程と、

を包含する方法。

２．安全なコンテンツ配送システムであって、

デジタル情報の少なくとも一部を暗号化する暗号化手段と、

１つまたはそれ以上のデジタルコンテナ内にデジタル情報をカプセル化し、インタラクションを管理するための少なくとも部分的に安全な制御情報と、該暗号化されたデジタル情報とを関連づけるコンテナ処理手段と、

該１つまたはそれ以上のデジタルコンテナの１つまたはそれ以上をデジタル情報ユーザに配送する配送手段と、

該デジタル情報の少なくとも一部の復号化を安全に制御する少なくとも１つの保護された処理環境と、

を有するシステム。

３．安全なデジタル情報配送方法であって、（ａ）該デジタル情報の少なくとも一部を第１の少なくとも１つのVDEノードを用いて暗号化する工程と、（ｂ）複数のユーザによる該デジタル情報の少なくとも一部の使用を制御する制御情報を、

該第１の少なくとも１つのVDEノードを用いて作成および暗号化する工程と、（

ｃ）該制御情報を該複数のユーザに安全に提供する工程と、（ｄ）該第１の少なくとも１つのVDEノードとは異なる少なくとも１つのVDEノードを用いて、該制御情報の少なくとも部分を処理し、該ユーザによる該暗号化されたデジタル情報の使用を制御する工程とによって特徴づけられる方法。

４．安全なデジタル情報配送システムであって、

該デジタル情報の少なくとも一部を暗号化する第１の少なくとも１つのVDEノードと、

複数のユーザによる該デジタル情報の少なくとも一部の使用を制御する制御情報を、該第１の少なくとも１つのVDEノードを用いて作成および暗号化する手段と、

該制御情報を該複数のユーザに安全に提供する手段と、

該制御情報の少なくとも部分を処理し、該ユーザによる該暗号化されたデジタル情報の使用を制御する該第１の少なくとも１つのVDEノードとは異なる少なくとも１つのVDEノードと

によって特徴づけられるシステム。

５．少なくとも部分的に暗号化されたコンテンツが少なくとも１つのデジタルコンテナ内にカプセル化され、該デジタルコンテナがデジタル情報ユーザに配送される安全なコンテンツ配送方法であって、

該コンテナおよび／または該コンテンツとのインタラクションを管理するための少なくとも部分的に安全な制御情報と、該カプセル化されたコンテンツおよび／または該デジタルコンテナとを関連づける工程と、

該制御情報に少なくとも部分的に基づいて該暗号化されたコンテンツの少なくとも一部の復号化を安全に制御する保護された処理環境を使用する工程と、

によって特徴づけられる方法。

６．少なくとも部分的に暗号化されたコンテンツが少なくとも１つのデジタルコンテナ内にカプセル化され、該デジタルコンテナがデジタル情報ユーザに配送される安全なコンテンツ配送システムであって、

該情報とのインタラクションを管理するための少なくとも部分的に安全な制御

情報と、該カプセル化されたコンテンツおよび／または該デジタルコンテナとを関連づけるデータ構造と、

該制御情報に少なくとも部分的に基づいて該暗号化されたコンテンツの少なくとも一部の復号化を安全に制御する保護された処理環境と、

によって特徴づけられるシステム。

７．安全なデジタル情報配送方法であって、（ａ）該デジタル情報の少なくとも一部を暗号化する工程と、（ｂ）保護された制御情報と該デジタル情報の少なくとも一部とを関連づける工程と、（ｃ）該暗号化されたデジタル情報の少なくとも一部を第１のユーザに提供し、該暗号化されたデジタル情報の少なくとも一部の使用を該保護された制御情報の少なくとも一部を用いて少なくとも部分的に制御する工程によって特徴づけられ、該第１のユーザがさらに、（ａ）該暗号化されたデジタル情報の該少なくとも一部のコピーまたは（ｂ）該暗号化されたデジタル情報の少なくとも１つを第２のユーザに提供し、該第２のユーザがさらに、第３のユーザによる該暗号化されたデジタル情報の使用の制御に用いられる制御情報と、該暗号化されたデジタル情報とを関連づける方法。

８．安全なデジタル情報配送システムであって、

該デジタル情報の少なくとも一部を暗号化する手段と、

保護された制御情報と該デジタル情報の少なくとも一部とを関連づける手段と、

該暗号化されたデジタル情報の少なくとも一部を第１のユーザに提供する手段と、

該暗号化されたデジタル情報の少なくとも一部の使用を該保護された制御情報の少なくとも一部を用いて少なくとも部分的に制御する手段と、

該第１のユーザに、（ａ）該暗号化されたデジタル情報の該少なくとも一部のコピーまたは（ｂ）該暗号化されたデジタル情報の少なくとも１つを第２のユーザに提供することを許容する手段と、

該第２のユーザに、第３のユーザによる該暗号化されたデジタル情報の使用の制御に用いられる制御情報と、該暗号化されたデジタル情報とをさらに関連づけ

ることを許容する手段と、

によって特徴づけられるシステム。

9．安全なデジタル取引管理方法であって、

ａ）第１のロケーションでデジタル情報を暗号化する工程と、

ｂ）第１のパーティが、該情報の使用の少なくとも１つの結果を確実にするのに使用される少なくとも１つの制御と、該情報とを安全に関連づけることを可能にする工程と、

ｃ）１つまたはそれ以上の他のパーティが、該情報の使用の少なくとも１つの結果を確実にするのに使用される少なくとも１つの他の制御と、該情報とを安全に関連づけることを可能にする工程と、

ｄ）該情報の少なくとも一部を、該第１および他のロケーションのロケーションとは異なるロケーションにおいて該第１および他のパーティ以外のパーティに配布する工程と、

ｆ）該第３のロケーションにおいて該情報の少なくとも一部を復号化し、該情報の使用の該結果を確実にする工程と、

を包含する方法。

10．以下の機能を実行する相互接続された構造を有する安全なデジタル取引管理システムであって、

ａ）デジタル情報を暗号化する機能と、

ｂ）第１のパーティが、該情報の使用の少なくとも１つの結果を確実にするのに使用される少なくとも１つの制御と、該情報とを安全に関連づけることを可能にする機能と、

ｃ）１つまたはそれ以上の他のパーティが、該情報の使用の少なくとも１つの他の結果を確実にするのに使用される少なくとも１つの他の制御と、該情報とを

安全に関連づけることを可能にする機能と、

ｄ）該情報の少なくとも一部を、他のパーティに配布する機能と、

ｅ）該情報の少なくとも一部を復号化する機能と、

ｆ）該結果を安全に確実にする機能と、

を実行するシステム。

11．デジタル情報が第１のロケーションにおいて第１のパーティによって暗号化され、配布される安全なデジタル取引管理システムであって、

該第１のパーティが少なくとも第１の制御と該情報とを安全に関連づけることを可能にする第１の保護された処理環境と、

他のパーティが少なくとも他の制御と該情報とを安全に関連づけることを可能にする他の保護された処理環境と、

該第１および他の制御に少なくとも部分的に基づいて該情報の使用の少なくとも１つの結果を制御しながら該情報の少なくとも一部を復号化するさらに他の保護された処理環境と、

によって特徴づけられるシステム。

12．デジタル情報が第１のロケーションにおいて第１のパーティによって暗号化され、配布される安全なデジタル取引管理方法であって、以下の工程：

該第１のパーティが少なくとも第１の制御と該情報とを安全に関連づけることを可能にする工程と、

他のパーティが少なくとも他の制御と該情報とを安全に関連づけることを可能にする工程と、

該第１および他の制御を送信する工程と、

該送信された制御に少なくとも部分的に基づいて少なくとも１つの結果を制御しながら該情報の少なくとも一部を復号化する工程と、

によって特徴づけられる方法。

13．配布された電子プロセスを安全に自動化する方法であって、

ａ）安全で相互作用可能な汎用の権利管理処理手段を多数のパーティに提供する工程と、

ｂ）電子イベントに関連する要件を自動的で、少なくとも部分的には遠隔に、および安全に支持するための安全なプロセス管理制御を確立する工程と、

ｃ）プロセス管理制御をパーティサイトに安全に配布する工程と、

ｄ）該パーティサイトにおいてパーティ処理手段の制御下で該プロセス管理制

御の少なくとも一部を安全に維持する工程と、

ｅ）該パーティサイトにおいて電子プロセスを自動的に管理し、該電子コンテンツに関連する利益を実施する工程と、

を包含する方法。

14．配布された電子プロセスを安全に自動化するシステムであって、

多数のパーティサイトに配置された相互作用可能な権利管理処理手段と、

安全なプロセス管理制御を確立し、電子イベントに関連する要件を遠隔、自動的、および安全に支持し、プロセス管理制御をパーティサイトに安全に配布する制御確立手段と、

該パーティサイトにおいて処理手段の制御下で該プロセス管理制御の少なくとも一部を安全に維持するセキュリティ手段と、

複数のパーティサイトにおいて電子プロセスを自動的に管理し、該電子イベントに関連する利益を実施する管理手段と、

を有するシステム。

15．多数のサイトにおいて相互作用可能なプロセッサを用いて配布された電子プロセスを自動化する方法であって、以下の工程：

電子イベントに関連する要件を自動的および安全に支持するためのプロセス管理制御を該プロセッサに安全に配布する工程と、

該プロセッサの制御下で該プロセス管理制御の少なくとも一部を安全に維持する工程と、

該多数のサイトにおいて電子プロセスを該プロセッサを用いて配布された様式で自動的に管理し、電子イベントに関連する利益を実施する工程と、

によって特徴づけられる方法。

16．多数のサイトにおいて相互作用可能なプロセッサを用いて配布された電子プロセスを自動化するシステムであって、以下の工程：

電子イベントに関連する要件を遠隔、自動的および安全に支持するためのプロセス管理制御をプロセッサに安全に配布する該プロセッサに接続された配布手段と、

該プロセッサの制御下で該プロセス管理制御の少なくとも一部を安全に維持するプロセス制御手段と、

該多数のサイトにおいて電子プロセスを該プロセッサを用いて配布された様式で自動的に管理し、該電子イベントに関連する利益を実施する管理手段と、

によって特徴づけられるシステム。

17. 権利順序判定システムを安全に実施する方法であって、

第１のユーザが電子コンテンツに対する少なくとも１つの制御を作成することを許容する工程と、

第２のユーザが電子コンテンツに対する少なくとも１つの他の制御を提供し、および／または該制御を適切に変更することを許容する工程であって、該第２の制御が該第１の制御の支配下にある工程と、

によって特徴づけられる方法。

18. 権利順序判定システムを安全に実施するシステムであって、

第１のユーザが電子コンテンツに対する少なくとも１つの制御を提供することを許容する第１の安全な環境と、

第２のユーザが電子コンテンツに対する少なくとも１つの他の制御を提供し、および／または該制御を適切に変更することを許容する第２の安全な環境であって、該第２の制御が該第１の制御の支配下にある第２の安全な環境と、

によって特徴づけられるシステム。

19. 第２のユーザが電子コンテンツの使用および／または該電子コンテンツへのアクセスに対する他の電子制御を作成しなければならない権利を少なくとも部分的に指図する少なくとも１つの電子制御を第１のユーザが作成することを許容する工程によって特徴づけられる権利順序判定システムを安全に実施する方法。

20. 第２のユーザが電子コンテンツの使用および／または該電子コンテンツへのアクセスに対する他の電子制御を作成しなければならない権利を少なくとも部分的に指図する少なくとも１つの電子制御を第１のユーザが作成することを許容する少なくとも１つの手段によって特徴づけられる権利順序判定システムを安全に実施するシステム。

２１．保護された処理環境を使用する方法であって、

ａ）相互作用可能な保護された処理環境を複数のパーティに配布する工程と、

ｂ）第１のパーティによって使用される第１の相互作用可能な保護された処理環境を提供し、該パーティが（ａ）デジタル情報を暗号化し、（ｂ）該デジタル情報の使用の少なくとも１つの局面を管理するための制御情報を作成することを可能にする工程と、

ｃ）該第１のパーティからの１つまたはそれ以上の命令に応答して該デジタル情報を暗号化する工程と、

ｄ）該デジタル情報を第２のパーティが得られるようにする工程と、

ｅ）第２の相互作用可能な保護された処理環境を用いて、該制御情報によって実施される要件を満足し、該第２のパーティが該デジタル情報の少なくとも一部を使用することを許容する工程と、

ｆ）該第２の相互作用可能な保護された処理環境を用いて、該デジタル情報の該第２のパーティによる使用の少なくとも１つの局面を反映する情報を安全に報告する工程と、

を包含する方法。

２２．保護された処理環境を使用するシステムであって、

複数のパーティに配布される相互作用可能な保護された処理環境であって、第１のパーティが（ａ）デジタル情報を暗号化し、（ｂ）該デジタル情報の使用の少なくとも１つの局面を管理するための制御情報を作成することを可能にする該第１のパーティによって使用される第１の相互作用可能な保護された処理環境を有し、第２の相互作用可能な保護された処理環境をさらに有する、相互作用可能な保護された処理環境と、

該第１のパーティからの１つまたはそれ以上の命令に応答して該デジタル情報を暗号化し、該デジタル情報を第２のパーティが得られるようにする手段と、

第２の相互作用可能な保護された処理環境を用いて、該制御情報によって実施される要件を満足し、該第２のパーティが該デジタル情報の少なくとも一部を使用することを許容し、該デジタル情報の該第２のパーティによる使用の少なくと

も１つの局面を反映する情報を安全に報告する手段と、

を有するシステム。

23. 複数のパーティに配布される保護された処理環境を使用する方法であって、以下の工程：

第１の保護された処理環境を用いて、デジタル情報および該デジタル情報の使用の少なくとも１つの局面を管理するための要件を指定する制御情報を暗号化する工程と、

該第１の保護された処理環境と相互作用可能な第２の保護された処理環境を用いて、該制御情報によって指定される該要件を実施し、該デジタル情報の少なくとも一部の使用を条件付きで可能にする工程と、

該第２の保護された処理環境を用いて、該デジタル情報の使用の少なくとも１つの局面を反映する情報を報告する工程と、

によって特徴づけられる方法。

24. 複数のパーティに配布される保護された処理環境を使用するシステムであって、

デジタル情報を暗号化し、該デジタル情報の使用の少なくとも１つの局面を管理するための要件を指定する制御情報を取り扱う第１の保護された処理環境と、

該制御情報によって指定される少なくとも１つの要件を実施し、該デジタル情報の少なくとも一部の使用を条件付きで可能にし、該デジタル情報の使用の少なくとも１つの局面を反映する情報を報告する、該第１の保護された処理環境と相互作用可能な第２の保護された処理環境と、

によって特徴づけられるシステム。

25. 保護された処理環境を備えた多数の協働する相互接続されたノードを有する安全なネットワークアーキテクチャであって、該ノードの少なくとも一部が相互通信可能であり、VDE保護下の情報が、ソースノードから行先ノードに移動され、該行先ノードによって少なくとも部分的に処理され得ることによって特徴づけられる安全なネットワークアーキテクチャ。

26. 保護された処理環境を備えた多数の協働する相互接続されたノードを有する

安全なネットワークアーキテクチャにおいて、該ノードが相互通信可能であり、VDE保護下の情報を、ソースノードから行先ノードに移動させ、該行先ノードによって少なくとも部分的に処理する工程を包含する方法。

27. 多数の協働する相互接続されたノードを有する安全なローカルエリアネットワークトポロジーであって、該ノードの少なくともいくつかがネットワークワークステーションを有し、ソフトウェアが保護された処理環境を定義し、該ノードの少なくとも１つが、該ネットワークワークステーション保護処理環境によって保護された形式で処理される情報を提供する安全なデータベースサーバを有することによって特徴づけられる安全なローカルエリアネットワークトポロジー。

28. 多数の協働する相互接続されたノードを有する安全なローカルエリアネットワークトポロジーにおいて、

保護された処理環境を定義するソフトウェアを、少なくとも部分的にネットワークワークステーションを用いて実行する工程と、

安全なデータベースサーバを用いて、該ネットワークワークステーション保護された処理環境によって処理される情報を提供する工程と、

によって特徴づけられる方法。

29. 保護された処理環境を備えた複数のノードを有する分散された電子権利管理システムであって、該複数のノードの少なくとも１つが、少なくとも１つの他のノードの該保護された処理環境の少なくとも一部を有するクライアントに対するサーバ機能を実施する保護された処理環境を提供することによって特徴づけられる分散された電子権利管理システム。

30. 保護された処理環境を備えた複数のノードを有する分散された電子権利管理システムにおいて、該複数のノードの少なくとも１つを用いて、保護された処理環境を提供する工程と、該保護された処理環境を用いて、少なくとも１つの他のノードの該保護された処理環境の少なくとも一部を有するクライアントに対するサーバ機能を実施する工程とによって特徴づけられる方法。

31. 電子商取引値チェーン活動に関連する電子ネゴシエーションを安全に管理する方法であって、

ａ）第１のパーティによって保護された処理環境を使用し、電子商取引プロセスを管理するための規則および／または制御を安全に指定する工程と、

ｂ）該指定された規則および／または制御が第２のパーティに安全に得られるようにする工程と、

ｃ）該第１の保護された処理環境とは異なる保護された処理環境を使用し、該第１のパーティおよび該第２のパーティの共通の商取引利益に関連する少なくとも１つの商取引プロセスを管理するための規則および／または制御をさらに安全に指定する工程と、

ｄ）該保護された処理環境を使用し、該第１のパーティおよび該第２のパーティの両方の電子利益を示すように設定された少なくとも１つの合計規則および／または制御を安全に電子的にネゴシエートする工程と、

ｅ）保護された処理環境を使用し、該設定された合計規則および／または制御の少なくとも一部と一致した該電子商取引プロセスを管理する工程と、

を包含する方法。

32．電子商取引値チェーン活動に関連する電子ネゴシエーションを安全に管理するシステムであって、

電子商取引プロセスを管理するための規則および／または制御を安全に指定し、該指定された規則および／または制御が第２のパーティに安全に得られるようにする第１のパーティの保護された処理環境と、

該第１のパーティおよび該第２のパーティの共通の商取引利益に関連する少なくとも１つの商取引プロセスを管理する手段を有する規則および／または制御をさらに安全に指定する、該第１のパーティの保護された処理環境とは異なる第２のパーティの保護された処理環境と、

該第１のパーティおよび該第２のパーティの両方の電子利益を示すように設定された少なくとも１つの合計規則および／または制御を安全に電子的にネゴシエートする該第１のパーティおよび該第２のパーティの保護された処理環境の少なくとも１つと、

該設定された合計規則および／または制御の該少なくとも一部と一致した該電

子商取引プロセスを管理する手段を有する、該第１のパーティおよび該第２のパーティの保護された処理環境の少なくとも１つと、

を有するシステム。

33．第１および第２の保護された処理環境を用いることによって、電子商取引値チェーン活動に関連する電子ネゴシエーションを安全に管理する方法であって、

該第１の環境を用いて、電子商取引プロセスを管理するための規則および／または制御を安全に指定する工程と、

該第２の環境を用いて、第１および第２のパーティの商取引利益に関連する少なくとも１つの商取引プロセスを管理するための規則および／または制御をさらに安全に指定する工程と、

該第１および第２の保護された処理環境の少なくとも１つを用いて、該第１のパーティおよび該第２のパーティの電子利益を示すように設定された少なくとも１つの合計規則および／または制御を安全に電子的にネゴシエートする工程と、

該第１および第２の保護された処理環境の少なくとも１つを用いて、該設定された合計規則および制御の少なくとも一部と一致した該電子商取引プロセスを管理する工程と、

によって特徴づけられる方法。

34．第１および第２の保護された処理環境を用いることによって、電子商取引値チェーン活動に関連する電子ネゴシエーションを安全に管理するシステムであって、

電子商取引プロセスを管理するための規則を安全に指定する手段を有する該第１の環境と、

第１および第２のパーティの商取引利益に関連する少なくとも１つの商取引プロセスを管理するための規則をさらに安全に指定する手段を有する該第２の環境と、

該第１のパーティおよび該第２のパーティの電子利益を少なくとも部分的に示すように設定された少なくとも１つの合計規則を安全に電子的にネゴシエートする手段を有する該第１および第２の保護された処理環境の少なくとも１つと、

該設定された合計規則の該少なくとも一部と一致した該電子商取引プロセスを管理する手段を有する該第１および第２の保護された処理環境の少なくとも１つと、

によって特徴づけられるシステム。

35. 分散された電子商取引環境を管理する方法であって、

ａ）電子商取引参加者に対するユーザＩＤを認証する安全な証明機関を確立する工程であって、該ＩＤが１つまたはそれ以上のユーザクラスパラメータを有する、工程と、

ｂ）該証明機関によって有効になった１つまたはそれ以上の証明書を用いて該ユーザＩＤを証明する工程と、

ｃ）該証明されたＩＤに含まれるクラスパラメータ情報に少なくとも部分的に基づいて配布された電子情報の使用を制御する工程と、

を包含する方法。

36. 分散された電子商取引環境を安全に管理するシステムであって、

電子商取引参加者に対するユーザＩＤを確立する手段であって、該ＩＤが１つまたはそれ以上のユーザクラスパラメータを有する、手段と、

該証明機関によって有効になった１つまたはそれ以上の証明書を用いて該ユーザＩＤを証明することによって該ユーザＩＤを認証する証明機関と、

該証明されたＩＤに含まれるクラスパラメータ情報に少なくとも部分的に基づいて配布された電子情報の使用を制御する手段と、

を有するシステム。

37. 分散された電子商取引環境を安全に管理し、証明機関によって証明されるユーザＩＤを有する電子商取引参加者とのインタラクションを可能にする方法であって、

ユーザＩＤを確立する工程と、

該ユーザＩＤおよびユーザクラスパラメータを証明する工程と、

少なくとも１つのユーザクラスパラメータと該ユーザＩＤとを関連づける工程であって、該証明されたクラスパラメータが、配布された電子情報の使用を制御す

るために少なくとも部分的に用いられる工程と、

によって特徴づけられる方法。

38. 分散された電子商取引環境を管理し、証明されたユーザIDを有する電子商取引参加者とのインタラクションを可能にするシステムであって、

少なくとも１つのユーザクラスパラメータと確立されたユーザIDとを関連づける手段と、

該ユーザIDおよび／または該ユーザクラスパラメータの認証性を確かめる手段と、

該ステータスに少なくとも部分的に基づいて配布された電子情報の使用を制御する手段と、

によって特徴づけられるシステム。

39. 前記クラスパラメータが、ユーザの年齢を示し、前記制御手段が、該ユーザの年齢に基づいて配布された電子情報の使用を制御する手段を有する、請求項38に記載のシステム。

40. 証明書を用いることによってユーザIDを安全に確立する方法であって、

少なくとも１つのユーザクラス特性を反映する電子トークンを示す工程と、

電子証明書が該トークンによって反映される該ユーザクラス特性を認証するか否かを決定する工程と、

該トークンを権利を交付するための根拠として使用する工程と、

によって特徴づけられる方法。

41. 証明書を用いることによってユーザを同定するシステムであって、

少なくとも１つのユーザクラス特性を反映する電子トークンを示す手段と、

電子証明書を得る手段と、

該電子証明書が該トークンによって反映される該ユーザクラス特性を認証するか否かを決定する手段と、

該証明され認証されたトークンを権利を交付するための根拠として使用する手段と、

によって特徴づけられるシステム。

42. 分散された電子商取引環境を安全に管理するシステムであって、

少なくとも１つのユーザカテゴリーを指定することによって電子商取引参加者を同定する手段と、

該ユーザIDを認証する手段と、

該ユーザカテゴリーに少なくとも部分的に基づいて配布された電子情報の使用を制御する手段と、

を有するシステム。

43. 電子商取引参加者とのインタラクションを可能にするために分散された電子商取引環境を安全に管理する方法であって、

ユーザIDおよび関連づけられたユーザクラスパラメータを確立する工程と、

該クラスパラメータを用いて、配布された電子情報の使用を少なくとも部分的に制御する工程と、

によって特徴づけられる方法。

44. 電子商取引参加者とのインタラクションを可能にするために分散された電子商取引環境を管理するシステムであって、

少なくとも１つのユーザクラスパラメータとユーザIDとを関連づける手段と、

該ユーザIDおよび／または該ユーザクラスパラメータを認証する手段と、

該ステータスに少なくとも部分的に基づいて配布された電子情報の使用を制御する手段と、

によって特徴づけられるシステム。

45. 前記クラスパラメータが、ユーザの年齢を示し、前記制御手段が、該ユーザの年齢に基づいて配布された電子情報の使用を制御する手段を有する、請求項44に記載のシステム。

46. ユーザIDを安全に確立する方法であって、

少なくとも１つのユーザクラス特性を反映する電子トークンを示す工程と、

該トークンによって反映される該ユーザクラス特性が正当であるか否かを決定する工程と、

該トークンを権利を交付するための少なくとも部分的な根拠として用いる工程

と、

によって特徴づけられる方法。

47. ユーザIDを安全に確立するシステムであって、

少なくとも１つのユーザクラス特性を反映する電子トークンを示す手段と、

該トークンによって反映される該ユーザクラス特性を認証する手段と、

該認証されたトークンを権利を交付するための根拠として用いる手段と、

によって特徴づけられるシステム。

48. ユーザIDを認証する方法であって、

証明書リクエストおよび関連づけられたユーザIDを受け取る工程と、

ユーザクラス特性に基づいて権利を交付するための該ユーザIDと関連づけられた少なくとも１つの該ユーザクラス特性を認証するのに用いられる電子証明書を発行する工程と、

によって特徴づけられる方法。

49. ユーザIDを認証するシステムであって、

証明書リクエストおよび関連づけられたユーザIDを受け取る手段と、

ユーザクラス特性に基づいて権利を交付するための該ユーザIDと関連づけられた少なくとも１つの該ユーザクラス特性を認証するのに用いられる電子証明書を発行する手段と、

によって特徴づけられるシステム。

50. ユーザIDを安全に確立する方法であって、

証明書リクエスト+を受け取る工程と、

少なくとも１つのユーザクラス特性を指定する電子証明書を発行する工程と、

によって特徴づけられる方法。

51. 証明書を用いることによってユーザIDを安全に確立するシステムであって、

証明書リクエストおよび関連づけられたユーザIDを受け取る手段と、

少なくとも１つのユーザクラス特性を指定する電子証明書を発行する手段と、

によって特徴づけられるシステム。

52. 権利を管理する方法またはシステムであって、暗号によって署名されたトークンがクラスにおけるメンバーシップを証明するために用いられ、該トークンが認証され、該トークンによって示される該クラスメンバーシップが、権利および／またはパーミッションを交付および／または差し押さえるための根拠として用いられることによって特徴づけられる方法またはシステム。

53. 権利を管理する方法またはシステムであって、暗号によって署名されたトークンがクラスにおけるメンバーシップを証明するために用いられ、該トークンのステータスが確かめられ、該トークンによって示される該クラスメンバーシップが、該トークンを示すユーザに電子規則を作成させるための根拠として使用されることによって特徴づけられる方法またはシステム。

54. 権利を管理する方法またはシステムであって、暗号によって署名されたトークンがクラスにおけるメンバーシップを証明するために用いられ、該トークンが有効性を検査され、該トークンによって示される該クラスメンバーシップが、該トークンを示すユーザに電子規則下で権利を行使させるための根拠として使用されることによって特徴づけられる方法またはシステム。

55. 分散された電子商取引電子契約システムを有効にする方法であって、

ａ）配布された、相互作用可能な安全なクライアント保護下の処理環境ノードを有効にする工程と、

ｂ）少なくとも１つのシステムワイドの安全な通信鍵を確立する工程と、

ｃ）複数のクライアントノード間の通信のための公開鍵暗号化を用いる工程と、

ｄ）個々のクライアントによる電子制御情報の配送を支持する工程であって、該制御情報が、それぞれの電子商取引契約権利を少なくとも部分的に指定する、工程と、

ｅ）該電子制御情報の安全な配送に少なくとも部分的に基づいて１つまたはそれ以上の電子契約を確立することによって、該クライアントのそれぞれのおよび／または集合的な権利を決定する少なくとも１つの保護された処理環境を支持する工程と、

ｆ）該クライアントの該電子権利の持続的な維持を確実にする安全なソフトウェアコンテナデータ制御構造を用いる工程と、

ｇ）電子商取引モデル契約実施に対応する規則および／または制御を支持するデータ構造を提供する安全なソフトウェアコンテナを用いる工程と、

を包含する方法。

56．分散された電子契約システムであって、

個々のクライアントによる電子制御情報の配送を支持し、該制御情報が該クライアントのそれぞれの電子商取引モデル契約権利を少なくとも部分的に指定し、該複数のクライアントノード間の通信のために公開鍵暗号化および認証を用いる複数の配布された相互作用可能な安全なクライアント保護下の処理環境ノードと、

該ノードに連結された、少なくとも１つのシステムワイドの安全な通信鍵を確立する手段と、

（ａ）該電子制御情報の安全な配送に少なくとも部分的に基づいて１つまたはそれ以上の電子契約を確立することによって、電子商取引モデルクライアントのそれぞれのおよび／または集合的な権利を決定し、

（ｂ）商取引モデルクライアントの該電子権利の持続的な維持を確実にする安全なソフトウェアコンテナデータ制御構造を用い、および

（ｃ）電子商取引モデル契約実施に対応する制御を支持するデータ構造を提供する安全なソフトウェアコンテナを用いる

少なくとも１つの保護された処理環境と、

を有するシステム。

57．少なくとも１つのシステムワイドの安全な通信鍵を用い、複数のクライアントノード間の通信のために公開鍵暗号化および認証を用い、クライアントＩＤを確立する証明機関を用いる、配布された相互作用可能な安全なクライアント保護下の処理環境ノードを有する分散された電子商取引電子契約システムを有効にする方法であって、

電子商取引モデル契約権利制御情報の安全な配送を支持する工程と、

該電子制御情報の該安全な配送に少なくとも部分的に基づいて１つまたはそれ以上の電子契約を確立することによって、電子商取引モデルクライアントのそれぞれのおよび／または集合的な権利を決定する工程と、

該商取引モデルクライアントの該電子権利の遠隔で持続的な維持を確実にする安全なソフトウェアコンテナデータ制御構造を用いる工程と、

電子商取引モデル契約実施に対応する規則および制御を支持するデータ構造を提供する安全なソフトウェアコンテナを用いる工程と、

によって特徴づけられる方法。

58. 分散された電子商取引電子契約システムであって、

少なくとも１つのシステムワイドの安全な通信鍵を用い、複数のクライアントノード間の通信のために公開鍵暗号化および認証を用い、クライアントＩＤを確立する証明機関を用い、電子商取引モデル契約権利制御情報の安全な配送を支持する、配布された相互作用可能な安全なクライアント保護下の処理環境ノードと、

少なくとも１つのノード内に配置される、該電子制御情報の該安全な配送に少なくとも部分的に基づいて１つまたはそれ以上の電子契約を確立することによって電子商取引モデルクライアントのそれぞれのおよび／または集合的な権利を決定する手段と、

少なくとも１つのノード内に配置される、該商取引モデルクライアントの該電子権利の遠隔で持続的な維持を確実にする安全なソフトウェアコンテナデータ制御構造を用い、電子商取引モデル契約実施に対応する規則および制御を支持するデータ構造を提供する安全なソフトウェアコンテナを用いる手段と、

を有するシステム。

59. 電子通貨を安全に取り扱う方法であって、以下の工程：

ソフトウェアコンテナ内に電子通貨をパッケージする工程と、

該ソフトウェアコンテナを物資またはサービスの支払いとして配送する工程と

によって特徴づけられる方法。

60. 電子通貨を安全に取り扱うシステムであって、

ソフトウェアコンテナ内に電子通貨をパッケージする手段と、

該ソフトウェアコンテナを物資またはサービスの支払いとして配送する手段と

、

によって特徴づけられるシステム。

61．組織内の権利を管理する方法またはシステムであって、電子コンテナが該組織内で配布され、該電子コンテナが該電子コンテナと関連づけられた制御を有し、該制御が該コンテナおよび／または該コンテナのコンテンツの使用に関連する組織的階層を少なくとも部分的に実施する方法またはシステム。

62．組織的な権利管理方法であって、

組織内に電子コンテナを配布する工程と、

該電子コンテナと関連づけられた電子制御に基づいて、該組織内または該組織外での該電子コンテナまたは該電子コンテナのコンテンツの使用、アクセスおよび／またはさらなる配布を制限する工程と、

によって特徴づけられる方法。

63．組織的な権利管理システムであって、

電子コンテナを配布する手段と、

該電子コンテナと関連づけられた電子制御に基づいて、該組織内または該組織外での該電子コンテナまたは該電子コンテナのコンテンツの使用、アクセスおよび／またはさらなる配布を制限する手段と、

によって特徴づけられるシステム。

64．組織的な権利管理方法であって、

組織内に電子コンテナを配布する工程と、

該電子コンテナを用いて、該組織内の人々によるコンテンツの使用を少なくとも部分的に管理する工程と、

によって特徴づけられる方法。

65．組織的な権利管理システムであって、

組織内に電子コンテナを配布する手段と、

該電子コンテナを用いて、該組織内の人々によるコンテンツの使用を少なくと

も部分的に管理する手段と、

によって特徴づけられるシステム。

66. 組織的な権利管理方法であって、

組織内に電子コンテナを配布する工程と、

該電子コンテナを用いて、該組織内の金銭の使用を少なくとも部分的に管理する工程と、

によって特徴づけられる方法。

67. 組織内に配布され、該組織内の金銭の使用を少なくとも部分的に管理する電子コンテナによって特徴づけられる組織的な権利管理システム。

68. 組織的な権利管理方法であって、

組織内に保護された処理環境を配布する工程と、

該環境を用いて、該組織内の人々によるコンテンツの使用を少なくとも部分的に管理する工程と、

によって特徴づけられる方法。

69. 組織内に配布され、該組織内のコンテンツ使用を少なくとも部分的に管理する保護された処理環境によって特徴づけられる組織的な権利管理システム。

70. 組織的な権利管理方法であって、

組織内に保護された処理環境を配布する工程と、

該処理環境を用いて、該組織内の人々による金銭の使用を少なくとも部分的に管理する工程と、

によって特徴づけられる方法。

71. 組織的な権利管理システムであって、

組織内に配布され、該組織内の金銭の使用を少なくとも部分的に管理する複数の保護された処理環境によって特徴づけられるシステム。

72. ユーザ入力デバイスと、

ユーザ表示デバイスと、

少なくとも１つのプロセッサと、

保護された処理環境を定義する少なくとも１つの素子とを有し、

該保護された処理環境が、権利を電子的に管理するためのパーミッション、メソッド、鍵、プログラムおよび／または他の情報を格納および使用することによって特徴づけられる権利管理機器。

73. ユーザ入力デバイスと、

ユーザ表示デバイスと、

少なくとも１つのプロセッサと、

保護された処理環境を定義する少なくとも１つの素子と、

を有する権利管理機器において、

権利を電子的に管理するためのパーミッション、メソッド、鍵、プログラムおよび／または他の情報を格納および使用する工程によって特徴づけられる該機器を動作させる方法。

74. 保護された処理環境を少なくとも部分的に定義する少なくとも１つのプロセッサ素子を有する権利管理機器であって、該保護された処理環境が、権利を電子的に管理するためのパーミッション、メソッド、鍵、プログラムおよび／または他の情報を格納および使用することによって特徴づけられる権利管理機器。

75. 保護された処理環境を少なくとも部分的に定義する少なくとも１つのプロセッサ素子を有する権利管理機器において、権利を電子的に管理するためのパーミッション、メソッド、鍵、プログラムおよび／または他の情報を格納および使用する工程を包含する方法。

76. 格納場所内に情報を電子的に格納し、該情報をリクエストに応じて配布する方法であって、該情報が電子制御と該情報とを関連づけることによって保護され、該電子制御が該情報内の権利を実施するように作用することによって特徴づけられる方法。

77. 格納場所内に情報を電子的に格納し、該情報をリクエストに応じて配布するシステムであって、電子制御と該情報とを関連づけることによって情報を保護する手段によって特徴づけられ、該電子制御を用いて該情報内の権利を実施する手段をさらに有するシステム。

78. デジタル情報を収容する電子コンテナ構造と、

不正改変のときに該デジタル情報を保護または破壊する電子保護機構と、

を有する自己保護電子コンテナ。

79. デジタル情報を収容する電子コンテナ構造を有する自己保護電子コンテナの方法であって、不正改変のときにアテンプト（attempt）を検出し、該アテンプトにおける該デジタル情報を保護または破壊することによって特徴づけられる方法。

80. 自己保護コンテナシステムを作成する方法であって、

少なくとも１つのプロパティを提供する工程と、

少なくとも１つのアトリビュートを提供する工程と、

少なくとも１つの暗号化鍵を提供する工程と、

該鍵と該プロパティおよび／または該アトリビュートとを関連させる少なくとも１つの組織的な構造を提供する工程と、

該プロパティ、該アトリビュート、該暗号化鍵、および該組織的な構造を、明示的または参照によって、電子コンテナ構造にカプセル化する工程と、

を包含する方法。

81. 少なくとも１つのプロパティと、

少なくとも１つのアトリビュートと、

少なくとも１つの暗号化鍵と、

該鍵と該プロパティおよび／または該アトリビュートとを関連させる少なくとも１つの組織的な構造と、

を有する自己保護コンテナシステム。

82. 保護された処理環境を備えた複数のノードを有する分散された電子権利管理システムであって、各ノードが電子構成要素に応答して自己管理プロセスを実施し得ることによって特徴づけられるシステム。

83. 取引の少なくとも一部を実施する少なくとも１つのメソッドと、

監査情報を生成する少なくとも１つのメソッドと、

管理情報を安全に受け取り解釈する少なくとも１つのメソッドと、

を有する自己管理電子構成要素。

84．以下のメソッドを実施する自己管理電子構成要素であって、

取引の少なくとも一部を実施する少なくとも１つのメソッドと、

監査情報を生成する少なくとも１つのメソッドと、

管理情報を安全に受け取り解釈する少なくとも１つのメソッドと、

を行う自己管理電子構成要素。

85．少なくとも１つのパラメータおよび／または関数を定義する自己記述電子構成要素であって、該構成要素が、該パラメータおよび／または該関数を記述する人間可読のインターフェースを作成するために用いられる少なくとも１つの安全な記述部を有することによって特徴づけられる自己記述電子構成要素。

86．少なくとも１つのパラメータおよび／または関数を定義する自己記述電子構成要素を処理する方法であって、該構成要素の少なくとも１つの安全な記述部に少なくとも部分的に基づいて、該パラメータおよび／または該関数を記述する人間可読のインターフェースを、該構成要素を少なくとも部分的に用いて作成する工程によって特徴づけられる方法。

87．電子取引を行う方法であって、

複数の構成要素を受け取る工程と、

イベントの発生を電子的に検出する工程と、

該イベントに基づいて、該受け取った複数の構成要素のサブセットを決定し、該イベントを処理する工程と、

該イベントに応答して、該構成要素のサブセットに基づいて少なくとも１つの電子プロセスを実施する工程と、

を包含する方法。

88．電子取引を実施するシステムであって、

複数の構成要素を受け取る手段と、

イベントの発生を電子的に検出する手段と、

該イベントに基づいて、該受け取った複数の構成要素のサブセットを決定し、該イベントを処理する手段と、

該イベントに応答して、該構成要素のサブセットに基づいて少なくとも１つの

電子プロセスを実施する手段と、

を有するシステム。

89．以下の工程によって特徴づけられる分散された取引処理方法であって、

第１のロケーションにおいて第１の電子構成要素を受け取る工程と、

第２のロケーションにおいて第２の電子構成要素を受け取る工程と、

該第１のロケーションにおいてイベントの発生を電子的に検出する工程と、

該イベントの検出に応答して、該第１の電子構成要素に少なくとも部分的に基づいて該第１のロケーションにおいて電子取引の第１の部分を処理する工程と、

該第１のロケーションから該第２のロケーションに少なくとも１つの信号を安全に送信する工程と、

該第２の電子構成要素に少なくとも部分的に基づいて該第２のロケーションにおいて該電子取引の少なくとも第２の部分を処理する工程と、

によって特徴づけられる方法。

90．前記第２のロケーションから前記第１のロケーションに少なくとも１つの信号を送る工程と、

該第２のロケーションからの該信号の受信に少なくとも部分的に基づいて該第１のロケーションにおいて該電子取引の少なくとも第３の部分を実施する工程と、

によってさらに特徴づけられる、請求項89に記載の方法。

91．分散された取引処理システムであって、

第１の電子構成要素を受け取り、イベントの発生を電子的に検出し、該イベントの検出に応答して、該第１の電子構成要素に少なくとも部分的に基づいて該第１のロケーションにおいて電子取引の第１の部分を処理し、該第１のロケーションから第２のロケーションに少なくとも１つの信号を安全に送信する、該第１のロケーションにおける手段と、

第２の電子構成要素を受け取り、該第２の電子構成要素に少なくとも部分的に基づいて該電子取引の少なくとも第２の部分を処理する、該第２のロケーションにおける手段と、

によって特徴づけられるシステム。

92. 前記第２のロケーションから前記第１のロケーションに少なくとも１つの信号を送る、該第２のロケーションにおける手段と、

該第２のロケーションからの該信号の受信に少なくとも部分的に基づいて該第１のロケーションにおいて前記電子取引の少なくとも第３の部分を実施する、該第１のロケーションにおける手段と、

によってさらに特徴づけられる、請求項91に記載のシステム。

93. 保護された処理環境を備えた複数のノードを有する分散された電子権利管理システムであって、各ノードが電子構成要素の受け取りおよび組み立てに応答して電子プロセスを実施することが可能で、該ノードが該電子構成要素を組み立てる前に該電子構成要素のそれぞれを認証することによって特徴づけられるシステム。

94. 分散された電子権利管理方法であって、

少なくとも１つの保護された処理環境を用いて、電子構成要素の受け取りおよび組み立てに応答して電子プロセスを実施する工程と、

該保護された処理環境内で、該電子構成要素を組み立てる前に該電子構成要素のそれぞれを認証する工程と、

を包含する方法。

95. 前記認証する工程が、機関を証明することによって対応する証明書を得る工程を包含する、請求項94に記載の方法。

96. 保護された処理環境を備えた複数のノードを有する分散された電子権利管理システムであって、各ノードが電子構成要素の受け取りおよび組み立てに応答して電子プロセスを実施することが可能で、該ノードが機関を証明することによって対応する証明書を得ることによって該電子構成要素のそれぞれを認証することによって特徴づけられるシステム。

97. 保護された処理環境を備えた複数のノードを有する分散された電子権利管理システムにおいて、電子構成要素を組み立て、電子権利管理プロセスを実施しお

よび／または制御する前に、各ノードに該電子構成要素を認証させる証明書を発行する証明機関。

98. それぞれが保護された処理環境を備えた複数のノードを有する分散された電子権利管理システムにおいて、電子構成要素を組み立て、電子権利管理プロセスを実施しおよび／または制御する前に、各ノードに該電子構成要素を認証させる証明書を発行する工程によって特徴づけられる方法。

99. 保護された処理環境を備えた複数のノードを有する分散された電子権利管理システムであって、該ノードが、使用および／またはアクセス制御を実施し、ユーザからの補償および／または権利所持者への次の転送のための使用情報の他の処理を電子的に得ることが可能であることによって特徴づけられるシステム。

100. 保護された処理環境を備えた複数のノードを有する分散された電子権利管理システムにおいて、使用および／またはアクセス制御を実施し、ユーザからの補償および／または権利所持者への次の転送のための使用情報の他の処理を電子的に得る工程によって特徴づけられる方法。

101. それぞれが保護された処理環境を備えた複数のノードを有する分散された電子権利管理システムであって、各ノードが、多数の他のノードからの情報の受け取りに基づいて使用および／またはアクセス制御を実施することによって特徴づけられるシステム。

102. 保護された処理環境を用いて、多数の他のノードからの情報の受け取りに基づいて使用および／またはアクセス制御を実施する工程によって特徴づけられる分散された電子権利管理方法。

103. 保護された処理環境を備えた複数のノードを有する分散された電子権利管理システムであって、該ノードが、権利所持者を補償するために用いられる電子貸し方を関連づけられたユーザに少なくとも一時的に延長し得ることによって特徴づけられるシステム。

104. 保護された処理環境を備えた複数のノードを有する分散された電子権利管理システムにおいて、権利所持者を補償するために用いられる電子貸し方を関連づけられたユーザに少なくとも一時的に延長する工程によって特徴づけられる該

環境を動作させる方法。

105. それぞれが保護された処理環境を備えた複数のノードを有する分散された電子権利管理システムであって、電子的に保護された情報にアクセスする権利および／または該情報を使用する権利をユーザに対して交付する前に、該ノードが情報交換所からユーザに特有の電子貸し方保証をリクエストし、獲得することが可能であることによって特徴づけられるシステム。

106. それぞれが保護された処理環境を備えた複数のノードを有する分散された電子権利管理システムにおいて、電子的に保護された情報にアクセスする権利および／または該情報を使用する権利をユーザに対して交付する前に、情報交換所からユーザに特有の電子貸し方保証をリクエストし、獲得する工程によって特徴づけられる方法。

107. それぞれが保護された処理環境を備えた複数のノードを有する分散された電子権利管理システムであって、各ノードが、電子的に保護された情報にアクセスする権利および／または該情報を使用する権利をユーザに対して交付するための条件として、電子貸し方または借方取引を実施しおよび／またはリクエストすることが可能であるシステム。

108. それぞれが保護された処理環境を備えた複数のノードを有する分散された電子権利管理システムにおいて、電子的に保護された情報にアクセスする権利および／または該情報を使用する権利をユーザに交付するための条件として、電子貸し方または貸し方取引を実施しおよび／またはリクエストする工程によって特徴づけられる方法。

109. それぞれが保護された処理環境を備えた複数のノードを有する分散された電子権利管理システムであって、各ノードが、中央ロケーションに報告するためのユーザ活動の監査追跡を維持することが可能であり、該中央ロケーションが該監査追跡に基づいて該ユーザ活動を分析することによって特徴づけられるシステム。

110. それぞれが保護された処理環境を備えた複数のノードを有する分散された電子権利管理システムにおいて、

中央ロケーションに報告するためのユーザ活動の監査追跡を複数のロケーションにおいて維持する工程と、

該監査追跡に基づいて該ユーザ活動を該中央ロケーションにおいて分析する工程と、

によって特徴づけられる方法。

１１１．保護された処理環境を備えた複数のノードを有する分散された電子権利管理システムであって、該ノードが、ユーザ活動をモニタし、該ユーザ活動および／または該ユーザ活動と関連しないイベントとを関連づける電子制御に基づいて該関連しないイベントの発生を誘発することが可能であることによって特徴づけられるシステム。

１１２．前記関連しないイベントが、アプリケーションプログラムの起動である、請求項１１１に記載のシステム。

１１３．前記関連しないイベントが、安全なコンテナの使用である、請求項１１１に記載のシステム。

１１４．前記関連しないイベントが、前記保護された処理環境の使用である、請求項１１１に記載のシステム。

１１５．保護された処理環境を備えた複数のノードを有する分散された電子権利管理システムにおいて、該ノードにおいてユーザ活動をモニタし、該ユーザ活動および該ユーザ活動と関連しないイベントとを関連づける電子制御に基づいて該関連しないイベントの発生を誘発する工程によって特徴づけられる方法。

１１６．前記関連しないイベントが、

アプリケーションプログラムの起動、

安全なコンテナの使用、および

前記保護された処理環境の使用

の少なくとも１つである、請求項１１５に記載の方法。

１１７．保護された処理環境を備えた複数のノードを有する分散された電子権利管理システムを侵犯する方法であって、以下の工程：

証明書秘密鍵を明らかにし、人にチャレンジ／レスポンスプロトコルを実行さ

せる工程と、

（ａ）初期化チャレンジ／レスポンスセキュリティの少なくとも１つを破り、および／または（ｂ）外部通信鍵を明らかにする工程と、

上記の工程に少なくとも部分的に基づいて処理環境を作成する工程と、

該処理環境を用いて、配布された権利管理に関与する工程と、

によって特徴づけられる方法。

118. 保護された処理環境を備えた複数のノードを有する分散された電子権利管理システムを侵犯する処理環境であって、

チャレンジ／レスポンスプロトコルを実行させるための明らかにされた証明書

秘密鍵を有する手段と、

（ａ）初期化チャレンジ／レスポンスセキュリティの少なくとも１つを破り、および／または（ｂ）外部通信鍵を明らかにする手段と、

配布された権利管理に関与する手段と、

によって特徴づけられる処理環境。

119. 保護された処理環境を備えた複数のノードを有する分散された電子権利管理システムを侵犯する方法であって、電子コンテナのパーミッション記録を侵犯し、該侵犯されたパーミッション記録を用いて、電子情報にアクセスおよび／または該情報を使用する工程によって特徴づけられる方法。

120. 保護された処理環境を備えた複数のノードを有する分散された電子権利管理システムを侵犯するシステムであって、電子情報にアクセスおよび／または該情報を使用するための電子コンテナの侵犯されたパーミッション記録を用いる手段によって特徴づけられるシステム。

121. 保護された処理環境を不正改変する方法であって、

少なくとも１つのシステムワイド鍵を発見する工程と、

該鍵を用いて、アクセス権限なしにコンテンツおよび／または管理情報にアクセスする工程と、

によって特徴づけられる方法。

122. 少なくとも１つの侵犯されたシステムワイド鍵を用いて、承認なしに保護

された処理環境のコンテンツおよび／または管理情報を復号化および侵犯する手段を有する配置。

123. 保護された処理環境を備えた複数のノードを有する分散された電子権利管理システムであって、該ノードが、コンテンツを非保護形式で明らかにする前に該コンテンツを電子的に指紋刻印することが可能であることによって特徴づけられるシステム。

124. 保護された処理環境を備えた複数のノードを有する分散された電子権利管理システムにおいて、該ノードの少なくとも１つにおいて、コンテンツを非保護形式で明らかにする前に該コンテンツを電子的に指紋刻印する工程によって特徴づけられる方法。

125. 保護された処理環境を備えた複数のノードを有する分散された電子権利管理システムであって、該ノードが、コンテンツを電子コンテナに含ませるかまたは該コンテンツへのアクセスを可能にする前に、コンテンツ権利所持者および／または起源の指示を同定する指定された情報を含む電子指紋を該電子コンテンツ内に埋め込むことが可能であることによって特徴づけられるシステム。

126. 保護された処理環境を備えた複数のノードを有する分散された電子権利管理システムにおいて、コンテンツを電子コンテナに含ませるかまたは該コンテンツへのアクセスを可能にする前に、コンテンツ権利所持者および／または起源の指示を同定する情報を有する指定の情報を含む電子指紋を該電子コンテンツ内に埋め込む工程によって特徴づけられる方法。

127. 保護された処理環境を備えた複数のノードを有する分散された電子権利管理システムであって、該システムが、該複数のノードの１つまたはそれ以上から使用情報を受け取る１つまたはそれ以上の使用情報交換所を有することによって特徴づけられるシステム。

128. 保護された処理環境を備えた複数のノードを有する分散された電子権利管理システムにおいて、使用情報交換所を用いて該複数のノードの１つまたはそれ以上から使用情報を受け取る工程によって特徴づけられる方法。

129. 保護された処理環境を備えた複数のノードを有する分散された電子権利管

理システムであって、該システムが、該ノードの１つまたはそれ以上からのコンテンツの使用または該コンテンツへのアクセスに関連する金融情報を受け取る１つまたはそれ以上の金融情報交換所を有することによって特徴づけられるシステム。

130. 保護された処理環境を備えた複数のノードを有する分散された電子権利管理システムにおいて、１つまたはそれ以上の金融情報交換所を用いて該複数のノードの１つまたはそれ以上からの金融情報を受け取る工程によって特徴づけられる方法。

131. 保護された処理環境を備えた複数のノードを有する分散された電子権利管理システムであって、該システムが、該複数のノードの１つまたはそれ以上からの情報を受け取り、該受け取った情報を分析する１つまたはそれ以上の分析情報交換所を有することによって特徴づけられるシステム。

132. 保護された処理環境を備えた複数のノードを有する分散された電子権利管理システムにおいて、１つまたはそれ以上の分析情報交換所を用いて該複数のノードの１つまたはそれ以上からの情報を受け取り、該受け取った情報を分析する工程によって特徴づけられる方法。

133. 電子コンテンツの使用または該電子コンテンツへのアクセスに関連する情報を処理する方法であって、該情報が保護された処理環境を有する１つまたはそれ以上のノードから受け取られる方法。

134. コンテンツとのインタラクションのための貸し方を保護された処理環境ノードに提供する方法。

135. 保護された処理環境を備えた複数のノードを有する分散された電子権利管理システムであって、該システムが、権利および／またはパーミッション情報を

該複数のノードの１つまたはそれ以上に送信する１つまたはそれ以上の情報交換所を有することによって特徴づけられるシステム。

136. 保護された処理環境を備えた複数のノードを有する分散された電子権利管理システムにおいて、権利および／またはパーミッション情報を情報交換所から該複数のノードの１つまたはそれ以上に送信する工程によって特徴づけられる方

法。

137. 保護された処理環境を備えた複数のノードを有する分散された電子権利管理システムであって、該システムが、暗号化材料を該ノードの１つまたはそれ以上に定期的に送信する１つまたはそれ以上の情報交換所を有し、該暗号化材料が、満期となる暗号化材料を更新および／または置換することによって特徴づけられるシステム。

138. 保護された処理環境を備えた複数のノードを有する分散された電子権利管理システムにおいて、１つまたはそれ以上の情報交換所から該ノードの１つまたはそれ以上に暗号化材料を定期的に送信し、該暗号化材料が、満期となる暗号化材料を更新および／または置換する工程によって特徴づけられる方法。

139. 安全な電子コンテナであって、該コンテナが該コンテナの外部にある電子コンテンツの使用および／または該電子コンテンツへのアクセスを制御する電子制御を有することによって特徴づけられる安全な電子コンテナ。

140. 安全な電子コンテナ内の電子制御にアクセスする工程と、

該コンテナの外部にある電子コンテンツの使用および／または該電子コンテンツへのアクセスを少なくとも部分的に制御する制御を用いる工程と、

を包含する方法。

141. 安全な電子コンテナであって、該コンテナが配布された電子コンテンツの使用および／または該電子コンテンツへのアクセスを少なくとも部分的に制御する電子制御を有することによって特徴づけられる安全な電子コンテナ。

142. 安全な電子コンテナ内の電子制御にアクセスする工程と、

配布された電子コンテンツの使用および／または該電子コンテンツへのアクセスを少なくとも部分的に制御する制御を用いる工程と、

を包含する方法。

143. 安全な電子コンテナであって、該コンテナが時間依存ベースで電子コンテンツを満期にする電子制御を有することによって特徴づけられる安全な電子コンテナ。

144. 安全な電子コンテナを処理する方法であって、該コンテナ内の電子制御に

少なくとも部分的に基づいて電子コンテンツを時間依存ベースで満期にする工程を包含する方法。

145. 電子情報の使用および／または該電子情報へのアクセスを計量する方法であって、該計量情報を時間および／または主題で細別するデータパーティションを有するビットマップ計量器データ構造を維持する工程によって特徴づけられる方法。

146. 電子情報の使用および／または該電子情報へのアクセスを計量するシステムであって、該計量情報を時間および／または主題で細別するデータパーティションを有するビットマップ計量器データ構造を維持する手段によって特徴づけられるシステム。

147. 保護された処理環境を備えた複数のノードを有する分散された電子権利管理システムであって、該システムが該ノードの少なくともいくつかに電子コンテンツの許可された使用を安全に記述させ、該記述を安全に実施することによって

特徴づけられるシステム。

148. 保護された処理環境を備えた複数のノードを有する分散された電子権利管理システムにおいて、該ノードの少なくともいくつかに電子コンテンツの許可された使用を安全に記述させ、該記述を安全に実施する工程によって特徴づけられる方法。

149. １つまたはそれ以上の安全な処理ユニットおよび該安全な処理ユニットの少なくとも１つに操作によって接続される１つまたはそれ以上の安全なデータベースを含む１つまたはそれ以上の電子機器を有する文書管理システムであって、該システムは、さらに保護された使用制御情報を有し、（ａ）該制御情報の少なくとも一部が、該安全なデータベースの１つまたはそれ以上内に安全に格納され、（ｂ）該制御情報の少なくとも一部が、使用情報の製造を制御し、該使用情報の少なくとも一部が１つまたはそれ以上のパーティに報告されるシステム。

150. １つまたはそれ以上の安全な処理ユニットおよび該安全な処理ユニットの少なくとも１つに操作によって接続される１つまたはそれ以上の安全なデータベースを含む１つまたはそれ以上の電子機器を有する文書管理システムにおいて、

保護された使用制御情報を処理する方法であって、該制御情報の少なくとも一部を、該安全なデータベースの１つまたはそれ以上内に安全に格納する工程と、（ｂ）該制御情報に少なくとも部分的に基づいて、使用情報の製造を管理し、該使用情報の少なくとも一部を１つまたはそれ以上のパーティに報告する工程とを包含する方法。

151. 保護された処理環境および該保護された処理環境の少なくとも１つに操作によって接続される１つまたはそれ以上の安全なデータベースを含む複数の電子機器を有する文書管理システムであって、該システムは、さらに保護された使用制御情報を有し、（ａ）該制御情報の少なくとも一部が、該安全なデータベースの１つまたはそれ以上内に安全に格納され、（ｂ）該制御情報の少なくとも一部が、使用情報の製造および該使用情報の少なくとも一部の１つまたはそれ以上のパーティへの報告を管理するシステム。

152. 保護された処理環境および該保護された処理環境の少なくとも１つに操作によって接続される１つまたはそれ以上の安全なデータベースを含む複数の電子機器を有する文書管理システムにおいて、使用制御情報を取り扱う方法であって、（ａ）該安全なデータベースの１つまたはそれ以上内に該制御情報の少なくとも一部を安全に格納する工程と、（ｂ）該制御情報の少なくとも一部に基づいて、使用情報の製造および該使用情報の少なくとも一部の１つまたはそれ以上のパーティへの報告を制御する工程とを包含する方法。

153. １つまたはそれ以上の安全な処理ユニットおよび該安全な処理ユニットの少なくとも１つに操作によって接続される１つまたはそれ以上の安全なデータベースを含む電子機器を有する電子契約システムであって、該システムは、複数のパーティが電子配置に入ることを可能にする手段を有し、該データベースの少なくとも１つは、複数のパーティ電子配置の少なくとも一部を管理する安全な制御情報を含むシステム。

154. １つまたはそれ以上の安全な処理ユニットおよび該安全な処理ユニットの少なくとも１つに操作によって接続される１つまたはそれ以上の安全なデータベースを含む複数の電子機器を有する電子契約システムにおいて、複数のパーティ

が電子配置に入ることを可能にする工程と、複数のパーティ電子配置の少なくとも一部を管理する該データベースの少なくとも１つに含まれる安全な制御情報を用いる工程とによって特徴づけられる方法。

155．少なくとも１つの安全な処理ユニットおよび該安全な処理ユニットの少なくとも１つに操作によって接続される少なくとも１つの安全なデータベースを含む電子機器配置であって、機器使用の少なくとも１つの局面の使用をモニタし、保護された機器使用制御情報に少なくとも部分的に基づいて該使用を制御する手段を有する配置。

156．少なくとも１つの安全な処理ユニットおよび該安全な処理ユニットの少なくとも１つに操作によって接続される少なくとも１つの安全なデータベースを含む電子機器配置において、機器使用の少なくとも１つの局面の使用をモニタする工程と、保護された機器使用制御情報に少なくとも部分的に基づいて該使用を制御する工程とによって特徴づけられる方法。

157．保護された処理環境および該保護された処理環境に操作によって接続される少なくとも１つの安全なデータベースを含む電子機器配置であって、機器使用量の少なくとも１つの局面の使用をモニタし、該保護された処理環境を少なくとも部分的に用いて処理された保護された機器使用制御情報に少なくとも部分的に基づいて該使用を制御する手段を有する配置。

158．保護された処理環境および該保護された処理環境に操作によって接続される少なくとも１つの安全なデータベースを含む電子機器配置において、機器使用の少なくとも１つの局面の使用をモニタする工程と、該保護された処理環境を少なくとも部分的に用いて処理された保護された機器使用制御情報に少なくとも部分的に基づいて該使用を制御する工程とによって特徴づけられる方法。

159．１つまたはそれ以上のCPUを有する電子機器配置であって、該CPUの少なくとも１つが集積された安全な処理ユニットを備え、該配置が該集積された安全な処理ユニットによって安全に処理されるように設計された保護された機器使用制御情報を格納する配置。

160．１つまたはそれ以上のCPUを有する電子機器配置において、該CPUの少なく

とも１つが集積された安全な処理ユニットを備え、該集積された安全な処理ユニットを用いて保護されたモジュラ構成要素機器使用制御情報を格納し安全に処理する工程を包含する方法。

161. 少なくとも１つの第１の安全な処理ユニットおよび１つまたはそれ以上のビデオコントローラを有する電子機器配置であって、該ビデオコントローラの少なくとも１つが少なくとも１つの第２の安全な処理ユニットを備え、該配置が該備えられた安全な処理ユニットによって安全に処理されるように設計される保護されたビデオ機能制御情報を格納する配置。

162. 少なくとも１つの第１の安全な処理ユニットおよび１つまたはそれ以上のビデオコントローラを有する電子機器配置において、該ビデオコントローラの少なくとも１つが少なくとも１つの第２の安全な処理ユニットを備え、該備えられた安全な処理ユニットによって安全に処理されるように設計される保護されたビデオ機能制御情報を格納する工程によって特徴づけられる方法。

163. ビデオコントローラの少なくとも１つが少なくとも１つの安全な処理ユニットを備える１つまたはそれ以上の該ビデオコントローラを有する電子機器配置であって、該備えられた安全な処理ユニットによって安全に処理されるように設計される保護されたビデオ機能制御情報を格納し、該ビデオ機能制御情報の少なくとも一部が該少なくとも１つの安全な処理ユニットの少なくとも１つに操作によって接続される安全なデータベース内に格納される配置。

164. １つまたはそれ以上のビデオコントローラを有する電子機器配置において、該ビデオコントローラの少なくとも１つが少なくとも１つの安全な処理ユニットを備え、該備えられた安全な処理ユニットによって安全に処理されるように設計される保護されたビデオ機能制御情報を、該少なくとも１つの安全な処理ユニットの少なくとも１つに操作によって接続されるデータベース内に格納する工程を包含する方法。

165. １つまたはそれ以上のビデオコントローラおよび少なくとも１つの安全な処理ユニットを有する電子機器配置であって、該安全な処理ユニットによって安全に処理されるように設計される、構成要素、モジュラ保護されたビデオ機能制

御情報を格納し、該ビデオ機能制御情報の少なくとも一部が該少なくとも１つの安全な処理ユニットの少なくとも１つに操作によって接続される安全なデータベース内に格納される配置。

166. １つまたはそれ以上のビデオコントローラおよび少なくとも１つの安全な処理ユニットを有する電子機器配置において、該安全な処理ユニットによって安全に処理されるように設計される、構成要素、モジュラ保護されたビデオ機能制御情報を、該少なくとも１つの安全な処理ユニットの少なくとも１つに操作によって接続される安全なデータベース内に格納する工程を包含する方法。

167. 少なくとも１つの安全な処理ユニットおよび１つまたはそれ以上のネットワーク通信手段を有する電子機器配置であって、該ネットワーク通信手段の少なくとも１つが少なくとも１つの他の安全な処理ユニットを備え、該配置が該備えられた安全な処理ユニットによって処理されるように設計される保護されたネットワーク制御情報を格納する配置。

168. 少なくとも１つの安全な処理ユニットおよび１つまたはそれ以上のネットワーク通信手段を有する電子機器配置において、少なくとも１つの他の安全な処理ユニットを該ネットワーク通信手段の少なくとも１つに備える工程と、ネットワーク制御情報を該備えられた安全な処理ユニット内に少なくとも部分的に格納する工程と、該保護されたネットワーク制御情報を該安全な処理ユニットを用いて安全に処理する工程とによって特徴づけられる方法。

169. １つまたはそれ以上のモデムを有する電子機器配置であって、該モデムの少なくとも１つが少なくとも１つの安全な処理ユニットを備え、該配置が該備えられた安全な処理ユニットによって安全に処理されるように設計されるモジュラ、構成要素保護モデム制御情報を格納する配置。

170. １つまたはそれ以上のモデムを有する電子機器配置において、該モデムの

少なくとも１つが少なくとも１つの安全な処理ユニットを備え、モジュラ、構成要素保護モデム制御情報を該備えられた安全な処理ユニットによって安全に処理する工程によって特徴づけられる方法。

171. 少なくとも１つの安全な処理ユニットおよび１つまたはそれ以上のモデム

を有する電子機器配置であって、該モデムの少なくとも１つが少なくとも１つの他の安全な処理ユニットを備え、該配置が該備えられた安全な処理ユニットによって安全に処理されるように設計される保護されたモデム制御情報を格納する配置。

172. 少なくとも１つの安全な処理ユニットおよび１つまたはそれ以上のモデムを有する電子機器配置において、該モデムの少なくとも１つが少なくとも１つの他の安全な処理ユニットを備え、保護されたモデム制御情報を該備えられた安全な処理ユニット内で格納および安全に処理する工程を包含する方法。

173. 少なくとも１つの安全な処理ユニットおよび１つまたはそれ以上のCD-ROMデバイスを有する電子機器配置であって、該CD-ROMデバイスの少なくとも１つが少なくとも１つの他の安全な処理ユニットを備え、該配置が該導入された安全な処理ユニットによって安全に処理されるように設計される保護されたCD-ROM制御情報を格納する配置。

174. 少なくとも１つの安全な処理ユニットおよび１つまたはそれ以上のCD-ROMデバイスを有する電子機器配置において、該CD-ROMデバイスの少なくとも１つが少なくとも１つの他の安全な処理ユニットを備え、該備えられた安全な処理ユニット内で保護されたCD-ROM制御情報を格納し安全に処理する工程によって特徴づけられる方法。

175. １つまたはそれ以上のネットワーク通信手段を有する電子機器配置であって、該ネットワーク通信手段の少なくとも１つが少なくとも１つの安全な処理ユニットを備え、該配置が該備えられた安全な処理ユニットによって安全に処理されるように設計されるモジュラ、構成要素保護ネットワーク制御情報を格納する配置。

176. １つまたはそれ以上のネットワーク通信手段を有する電子機器配置において、該ネットワーク通信手段の少なくとも１つが少なくとも１つの安全な処理ユニットを備え、保護されたネットワーク制御情報を該備えられた安全な処理ユニットを用いて格納および安全に処理する工程によって特徴づけられる方法。

177. 保護された処理環境および該保護された処理環境に操作によって接続され

るデータベースを有するセットトップコントローラ配置であって、該保護された処理環境内の制御情報の少なくとも一部の処理に基づいて該コントローラの使用を制御する該制御情報をさらに有し、該制御情報の少なくとも一部が該データベース内に格納される配置。

178. 保護された処理環境および該保護された処理環境に操作によって接続されるデータベースを有するセットトップコントローラ配置において、（ａ）該保護された処理環境内の制御情報の少なくとも一部の処理に基づいて該コントローラの使用を制御する該セットトップコントローラ配置内の該制御情報を用いる工程と、該制御情報の少なくとも一部を該データベース内に格納する工程とによって特徴づけられる方法。

179. 電子ゲームの使用を制御する保護された処理環境を有する電子ゲーム配置であって、ゲーム使用制御情報と、該ゲームの少なくとも１つの少なくとも一部の使用の少なくともいくらかの局面を制御する使用制御情報を少なくとも部分的に格納する該保護された処理環境に操作によって接続されるデータベース手段と、保護された電子ゲームコンテンツを含む移動オブジェクトとを有する配置。

180. 電子ゲームの使用を制御する保護された処理環境を有する電子ゲーム配置において、

（ａ）ゲーム使用制御情報を、該保護された処理環境に操作によって接続されるデータベース手段内に含ませる工程と、

（ｂ）該ゲームの少なくとも１つの少なくとも一部の使用の少なくともいくらかの局面を、該格納された使用制御情報を少なくとも部分的に用いて制御する工程とを包含する方法。

181. 保護された電子ゲームコンテンツを含む移動オブジェクトの使用を制御する工程をさらに包含する、請求項178に記載の方法。

182. インタラクティブゲームの使用を制御する相互作用可能な保護された処理環境を有する電子ゲーム配置であって、保護されたゲーム使用制御情報と、ゲーム使用制御情報を少なくとも部分的に格納する、該保護された処理環境に操作によって接続されたデータベース手段とを有する配置。

183. 保護された処理環境を有する電子ゲーム配置において、

（ａ）保護されたゲーム使用制御情報を、該保護された処理環境に操作によって接続される安全なデータベース手段内に格納する工程と、

（ｂ）該格納されたゲーム使用制御情報に少なくとも部分的に基づいて、インタラクティブゲームの使用を制御する工程と、

を包含する方法。

184. ゲームの使用を制御する相互作用可能な保護された処理環境を有する電子ゲーム配置であって、構成要素、モジュラ、保護ゲーム使用制御情報を有し、該保護された制御情報の少なくとも一部が、少なくとも１つの電子値チェーン内にそれぞれの権利を確保する複数のパーティによって独立して提供された配置。

185. ゲームの使用を制御する相互作用可能な保護された処理環境を有する電子ゲーム配置において、

（ａ）構成要素、モジュラ、保護ゲーム使用制御情報を複数のパーティによって独立して提供する工程と、

（ｂ）該制御情報を用いて、少なくとも１つの電子値チェーン内に該複数のパーティのそれぞれの権利を確保する工程と、

を包含する方法。

186. マルチメディアの使用を制御する保護された処理環境を有する電子マルチメディア配置であって、構成要素、モジュラマルチメディア使用制御情報と、該マルチメディア使用制御情報を少なくとも部分的に格納する、該保護された処理環境に操作によって接続されるデータベース手段とを有する配置。

187. マルチメディアの使用を制御する保護された処理環境を有する電子マルチメディア配置において、マルチメディア使用制御情報を、該保護された処理環境に操作によって接続されるデータベース手段内に格納する工程と、該格納された制御情報を制御マルチメディアに使用する工程とを包含する方法。

188. マルチメディアの使用を制御する保護された処理環境を有する電子マルチメディア配置であって、マルチメディア使用制御情報と、該保護された処理環境に操作によって接続される、該マルチメディア使用制御情報を少なくとも部分的

に格納するデータベース手段と、配布されたマルチメディア電子コンテンツを含む保護された移動オブジェクトとを有する配置。

189. 保護された処理環境を有する電子マルチメディア配置において、マルチメディア使用制御情報を、該保護された処理環境に操作によって接続されるデータベース手段内に格納し、該格納された情報に少なくとも部分的に基づいて、配布されたマルチメディア電子コンテンツを含む保護された移動オブジェクトを制御する工程とによって特徴づけられる方法。

190. マルチメディアの使用を制御する相互作用可能な保護された処理環境を有する電子マルチメディア配置であって、構成要素、モジュラ、保護されたマルチメディア使用制御情報を有し、該保護された制御情報の少なくとも一部が、少なくとも１つの電子値チェーン内にそれぞれの権利を確保する複数のパーティによって独立して提供された配置。

191. 安全な処理ユニットをさらに有する、請求項188に記載のシステム。

192. 保護された処理環境を有する電子マルチメディア配置において、構成要素、モジュラ、保護されたマルチメディア使用制御情報の少なくとも一部を、少なくとも１つの電子値チェーンにおいてそれぞれの権利を確保する複数のパーティによって独立して提供する工程と、該使用制御情報を使用してマルチメディアの使用を制御する工程とを包含する方法。

193. 前記使用する工程が、安全な処理ユニット内で少なくとも部分的に実施される、請求項190に記載の方法。

194. 少なくとも１つのマイクロプロセッサと、メモリと、入力／出力手段と、情報を暗号化および／または復号化する少なくとも１つの回路と、暗号化および／または復号化関数を実施する該マイクロプロセッサの少なくとも１つと共に用いられる１つまたはそれ以上のソフトウェアプログラムとを有する、多重暗号化アルゴリズムを支持する集積回路。

195. 少なくとも１つのマイクロプロセッサと、メモリと、入力／出力手段とを有し、保護された処理環境を提供する、多重暗号化アルゴリズムを支持する安全な集積回路において、該マイクロプロセッサを用いて１つまたはそれ以上のソフ

トウェアプログラムの少なくとも一部を実行し、該集積回路内で暗号化および／または復号化関数を実施することによって特徴づけられる方法。

196. 少なくとも１つのマイクロプロセッサと、メモリと、少なくとも１つのリアルタイムクロックと、少なくとも１つの乱数発生器と、情報を暗号化および／または復号化する少なくとも１つの回路と、独立して配送されるおよび／または独立して配送可能な証明されたソフトウェアとを有する集積回路。

197. 少なくとも１つのマイクロプロセッサと、メモリと、入力／出力手段と、不正改変不可能なバリアと、権利オペレーティングシステムの少なくとも一部とを有する集積回路。

198. 少なくとも１つのマイクロプロセッサと、メモリと、入力／出力手段と、少なくとも１つのリアルタイムクロックと、不正改変不可能なバリアと、パワーの中断を該リアルタイムクロックの少なくとも１つに記録する手段とを有する集積回路。

199. 情報を圧縮する工程と、該圧縮された情報を第１のロケーションで暗号化する工程と、該暗号化された情報を１つまたはそれ以上の第２のロケーションに配布する工程と、不正改変不可能な集積回路を用いて該情報を最初に復号化し、次に圧縮解除する工程とによって特徴づけられる情報を配布する方法。

200. 情報を配布するシステムであって、

情報を圧縮する手段と、

該圧縮された情報を第１のロケーションで暗号化する手段と、

該暗号化された情報を１つまたはそれ以上の第２のロケーションに配布する手段と、

不正改変不可能な集積回路を用いて該情報を最初に復号化し、次に圧縮解除する手段と、

によって特徴づけられるシステム。

201. 配布されたイベントを安全に管理する方法であって、安全なイベント処理環境を１つまたはそれ以上のユーザに提供する工程と、第１の安全なイベント処

理環境を用いて、第１のユーザがイベント管理のための制御情報を指定することを可能にする工程と、第２の安全なイベント処理環境を用いて該イベントの処理を管理する工程とによって特徴づけられる方法。

202. 配布されたイベントを安全に管理するシステムであって、

第１のユーザがイベント管理のための制御情報を指定することを可能にする第１の安全なイベント処理環境と、

該第１のイベント処理環境と相互作用可能な、該イベントの処理を管理する第２の安全なイベント処理環境と、

によって特徴づけられるシステム。

203. 処理と制御の電子商取引チェーンを有効にする方法であって、第１および第２のパーティが、電子商取引値チェーンの動作に関連する要件を記述する保護されたモジュラ構成要素制御情報を独立して指定する工程によって特徴づけられる方法。

204. 処理と制御の電子商取引チェーンを有効にするシステムであって、第１および第２のパーティに、処理および制御の電子商取引値チェーンの動作に関連する要件を記述する保護されたモジュラ構成要素制御情報を独立して指定することを許可する手段と、該制御情報によって記述される該要件を安全に実施する手段とによって特徴づけられるシステム。

205. 第１および第２のパーティがデジタル情報の使用を管理する制御情報を独立して規定する工程によって特徴づけられる電子商取引を有効にする方法であって、該第１および第２のパーティが、該デジタル情報が処理と制御のチェーンを通して移動するのに伴って、該制御情報によって実施される持続的な権利を独立して維持する方法。

206. 電子商取引を有効にするシステムであって、

第１のパーティが、デジタル情報の使用を管理する制御情報を規定することを許容する手段と、

第２のパーティが、該デジタル情報の使用を管理する制御情報を規定することを許容する手段と、

該デジタル情報が１つのロケーションおよび／またはプロセスから他のロケーションおよび／またはプロセスに移動するのに伴って、該制御情報によって実施される持続的な権利を維持する処理と制御のチェーン手段と、

を有するシステム。

207. 電子権利の安全な維持方法であって、値チェーン内の複数のパーティが、該パーティの電子権利に関する制御情報を独立して安全に規定する第１の工程を包含し、該制御情報が、ソフトウェアコンテナ内に配布された電子情報の使用に関連する条件を実施するために用いられる方法。

208. 電子権利の安全な維持システムであって、

値チェーン内の複数のパーティに該パーティの電子権利に関する制御情報を独立して安全に規定することを許可する手段と、

該制御情報を用いて、ソフトウェアコンテナ内に配布された電子情報の使用に関連する条件を実施する手段と、

を有するシステム。

209. 保護された電子コンテンツの使用を安全に制御する方法であって、該コンテンツの使用に関連する少なくとも１つのイベントを、ユーザが該少なくとも１つのイベントを管理するための個別の制御情報配置間で選択し得るように管理するモジュラ個別の制御情報配置を支持する工程を包含する方法。

210. 保護された電子コンテンツの使用を安全に制御するシステムであって、該コンテンツの使用に関連する少なくとも１つのイベントを、ユーザが該少なくとも１つのイベントを管理するための個別制御情報配置間で選択し得るように管理

するモジュラ個別の制御情報配置を有するシステム。

211. 暗号化されたデジタル情報の使用を管理する個別のモジュラ制御構造を使用する方法であって、商取引値チェーン参加者が、（１）コンテンツイベント誘発、（２）監査、および（３）予算作成の２つまたはそれ以上の制御変数間の複数の関係を支持することを可能にする工程によって特徴づけられる方法。

212. 暗号化されたデジタル情報の使用を管理する個別のモジュラ制御構造を使用するシステムであって、商取引値チェーン参加者が、（１）コンテンツイベン

ト誘発、（２）監査、および（３）予算作成の２つまたはそれ以上の制御変数間の複数の関係を支持することを可能にする手段によって特徴づけられるシステム。

213．電子値チェーンに直接関与しないパーティが、安全な制御情報を与え、少なくとも１つの制御要件を実施することを可能にする処理と制御のチェーン方法であって、第１の値チェーン参加者がデジタル情報に関連づけられた制御情報を規定する第１の工程と、該直接関与しないパーティが、該関連づけられた制御情報を含む合計制御情報セットに含まれる安全な制御情報を独立して安全に与える第２の工程であって、該合計制御情報が、第２の値チェーン参加者による該デジタル情報の少なくとも一部の使用に関連する条件を少なくとも部分的に管理する第２の工程とによって特徴づけられる方法。

214．電子値チェーンに直接関与しないパーティが安全な制御情報を与え、少なくとも１つの制御要件を実施することを可能にする処理と制御のチェーンシステムであって、

第１の値チェーン参加者がデジタル情報に関連づけられた制御情報を規定することを許容する手段と、

該直接関与しないパーティが、該関連づけられた制御情報を含む合計制御情報セットに含まれる安全な制御情報を独立して安全に与えることを許容する手段と、

該合計制御情報に応答する、第２の値チェーン参加者による該デジタル情報の少なくとも一部の使用に関連する条件を少なくとも部分的に管理する手段とによって特徴づけられるシステム。

215．値チェーンパーティによって保持される特定の権利の管理を第２の値チェーンパーティに委譲する電子商取引制御情報管理方法であって、該第１のパーティが、１つまたはそれ以上の処理と制御のチェーン電子イベントに関連する該第１のパーティの権利の少なくとも一部を記述する安全な制御情報を規定する工程によって特徴づけられ、該第１のパーティが、該権利のいくらかまたはすべてを該第１のパーティのエージェントとして管理することを該第２のパーティに承認

する制御情報をさらに提供する方法。

216. 値チェーンパーティによって保持される特定の権利の管理を第２の値チェーンパーティに委譲する電子商取引制御情報管理システムであって、

該第１のパーティが、１つまたはそれ以上の処理と制御のチェーン電子イベントに関連する該第１のパーティの権利の少なくとも一部を記述する安全な制御情報を規定することを許容する手段と、

該第１のパーティが、該権利のいくらかまたはすべてを該第１のパーティの代理として管理することを第２のパーティに承認する制御情報をさらに提供することを許容する手段と、

によって特徴づけられるシステム。

217. 処理と制御の電子チェーンから生じる商取引イベントの課税を管理する方法であって、安全なデジタル情報をユーザに配布し、該デジタル情報を使用するための少なくとも１つの条件を制御する安全な制御情報を指定する第１の工程と、管理エージェンシーが、該商取引イベントのための税金支払いを自動的に管理する安全な制御情報を安全に独立して与える第２の工程とによって特徴づけられる方法。

218. 処理と制御の電子チェーンから生じる商取引イベントの課税を管理するシステムであって、

安全なデジタル情報をユーザに配布する手段と、

該デジタル情報を使用するための少なくとも１つの条件を制御する安全な制御情報を指定する手段と、

管理エージェンシーが、該商取引イベントのための税金支払いを自動的に管理する安全な制御情報を安全に独立して与えることを許容する手段とによって特徴づけられるシステム。

219. 電子イベントに関連するプライバシ権利を管理する方法であって、第１のパーティが、第２のパーティの少なくとも１つの不許可使用を防止することを記述する情報を含むデジタル情報を保護する第１の工程と、該保護されたデジタル情報の少なくとも一部の使用に関連する特定の制御情報を指定する第２の工程と

によって特徴づけられ、該制御情報が、該保護されたデジタル情報に含まれるパーソナルおよび／またはプロプライエタリ情報のプライバシおよび／または許可された使用に関連する該第２のパーティの少なくとも１つの権利を実施する方法。

220．電子イベントに関連するプライバシ権利を管理するシステムであって、

第１のパーティに、第２のパーティの少なくとも１つの不許可使用を防止することを記述する情報を含むデジタル情報を保護することを許可する手段と、

該保護されたデジタル情報の少なくとも一部の使用に関連する指定の制御情報を指定する手段と、

該制御情報を用いて、該保護されたデジタル情報に含まれるパーソナルおよび／またはプロプライエタリ情報のプライバシおよび／または許可された使用に関連する該第２のパーティの少なくとも１つの権利を実施する手段と、

によって特徴づけられるシステム。

221．電子イベントに関連するプライバシ権利を管理する方法であって、第１のパーティが、デジタル情報を少なくとも１つの不許可使用から保護し、該保護された情報を使用するための条件を確立するための特定の制御情報を規定する第１の工程と、該デジタル情報のユーザが、該デジタル情報の少なくとも一部の該ユーザの使用に関する情報の報告を制御する他の制御情報を規定する第２の工程とによって特徴づけられる方法。

222．電子イベントに関連するプライバシ権利を管理するシステムであって、

第１のパーティが、デジタル情報を少なくとも１つの不許可使用から保護し、該保護された情報を使用するための条件を確立するための特定の制御情報を規定することを許容する手段と、

該デジタル情報のユーザが、該デジタル情報の少なくとも一部の該ユーザの使用に関する情報の報告を制御する他の制御情報を規定することを許容する手段と、

によって特徴づけられるシステム。

223．電子処理および商取引を制御する安全な方法であって、相互作用可能な保

護された処理環境を配布し、該保護された処理環境の少なくとも一部によって使用されるように準備されたデジタルコンテンツおよび関連のコンテンツ制御情報を含むソフトウェアコンテナを該保護された処理環境の複数の受け手の間に巡回する工程によって特徴づけられ、該制御情報の少なくとも一部の安全な処理に少なくとも部分的に基づいて、少なくとも１つの保護された処理環境を用いて、該デジタルコンテンツの少なくともいくらかの使用を制御するさらなる工程を包含する方法。

224. 電子処理および商取引を制御する安全なシステムであって、

配布された相互作用可能な保護された処理環境と、

該保護された処理環境の少なくとも一部によって使用されるように準備されたデジタルコンテンツおよび関連のコンテンツ制御情報を含むソフトウェアコンテナを該保護された処理環境間に巡回する手段と、

該保護された処理環境の少なくともいくらかの中にある、該制御情報の少なくとも一部の安全な処理に少なくとも部分的に基づいて、該デジタルコンテンツの少なくともいくらかの使用を制御する手段と、

によって特徴づけられるシステム。

225. 安全な電子小売り環境を有効にする電子商取引ネットワーキング方法であって、VDE通信技術および安全なソフトウェアコンテナを用いて共にネットワーク化された、証明された制御情報と、スマートカードと、安全な処理ユニットと、小売りターミナル配置とをユーザに提供する工程によって特徴づけられる方法。

226. 安全な電子小売り環境を有効にする電子商取引ネットワーキングシステムであって、

スマートカードと、安全な処理ユニットと、小売りターミナル配置とを共にネットワーク化する手段と、

該スマートカードと、該安全な処理ユニットと、該小売りターミナル配置とを互いに、ならびにVDE通信技術および安全なソフトウェアコンテナと相互作用可能にする手段と、

によって特徴づけられるシステム。

227. 商取引活動においてユーザの権利を安全に管理する電子商取引器具を有効にする方法であって、物理デバイス内に収容されたVDEノードの少なくとも一部をユーザに提供する工程であって、該デバイスが、複数のパーティ間の安全かつ相互作用可能な取引活動を支持するホストシステムにおける接合コネクタと適合するように構成される工程によって特徴づけられる方法。

228. 商取引活動においてユーザの権利を安全に管理するシステムであって、ポータブルVDEノードの少なくとも一部を備え、複数のパーティ間の安全かつ相互作用可能な取引活動を支持するホストシステムにおける接合コネクタと適合するように構成される物理デバイスを有するシステム。

229. プログラム可能な電子商取引環境を有効にする方法であって、個別のモジュラ構成要素課金管理メソッド、予算作成管理メソッド、計量管理メソッド、および関連の監査管理メソッドを安全に処理する安全な商取引ノードを多数のパーティに提供する工程によって特徴づけられ、電子商取引イベント活動に応答して計量、監査、課金、および予算作成メソッドの誘発を支持する工程によってさらに特徴づけられる方法。

230. 安全な商取引ノードによって特徴づけられるプログラム可能な電子商取引環境であって、各ノードが、

個別のモジュラ構成要素課金管理メソッド、予算作成管理メソッド、計量管理メソッド、および関連の監査管理メソッドを安全に処理する手段と、

電子商取引イベント活動に応答して計量、監査、課金、および予算作成メソッドの誘発を支持する手段と、

を有する環境。

231. モジュラ標準化制御構成要素を備えた電子商取引システムであって、商取引参加者によって規定される電子商取引イベント制御命令および該商取引イベント制御命令の少なくとも一部を処理する１つまたはそれ以上の安全な処理ユニットを含む複数の電子機器を有し、該少なくとも１つの安全な処理ユニットによって使用される該制御命令の少なくとも一部を少なくとも部分的に安全に格納する

該安全な処理ユニットの少なくとも１つに操作によって接続される１つまたはそれ以上のデータベースをさらに有するシステム。

232．モジュラ標準化制御構成要素を備えた電子商取引システムであって、商取引参加者によって規定される電子商取引イベント制御命令および該商取引イベント制御命令の少なくとも一部を処理する１つまたはそれ以上の安全な処理ユニットを含む複数の電子機器を有するシステムにおいて、該安全な処理ユニットの少なくとも１つに操作によって接続される１つまたはそれ以上の安全なデータベースを提供し、該安全なデータベース内に該少なくとも１つの安全な処理ユニットによって使用される該制御命令の少なくとも一部を少なくとも部分的に安全に格納する工程によって特徴づけられる方法。

233．安全な処理ユニットの少なくとも１つと共に用いられる１つまたはそれ以上のデータベースに操作によって接続される１つまたはそれ以上の相互作用可能な安全な該処理ユニットを備えた複数の電子機器を有するコンテンツ配布システムであって、該１つまたはそれ以上のデータベースが（ａ）配布され暗号化されたデジタル情報を復号化するのに用いられる１つまたはそれ以上の復号化鍵と、（ｂ）該配布されたデジタル情報の使用の少なくとも１つの局面を反映する暗号化された監査情報とを含むシステム。

234．コンテンツ配布方法であって、

１つまたはそれ以上の相互作用可能な安全な処理ユニットを有する複数の電子機器を配布する工程と、

該器具を１つまたはそれ以上のデータベースに操作によって接続する工程と、

１つまたはそれ以上の復号化鍵を該１つまたはそれ以上のデータベース内に格納する工程と、

該復号化鍵を配布され暗号化されたデジタル情報を復号化するために用いる工程と、

該配布されたデジタル情報の使用の少なくとも１つの局面を反映する暗号化された監査情報を該１つまたはそれ以上のデータベース内に格納する工程と、

を包含する方法。

235．電子通貨システムであって、（ａ）保護された処理環境と、（ｂ）暗号化された電子通貨および該保護された処理環境の少なくとも１つによって使用可能となるように構成された関連の安全な制御情報と、（ｃ）第１の相互作用可能な保護された処理環境からの電子通貨使用関連情報を、第２の相互作用可能な保護された処理環境に安全に通信させる使用報告手段とを備えた複数の電子機器を有するシステム。

236．電子通貨方法であって、

（ａ）保護された処理環境と、（ｂ）暗号化された電子通貨および該保護された処理環境の少なくとも１つによって使用可能となるように構成された関連の安全な制御情報とを備えた複数の電子機器を配布する工程と、

第１の相互作用可能な保護された処理環境からの電子通貨使用関連情報を、第２の相互作用可能な保護された処理環境に安全に通信させる工程と、

を包含する方法。

237．電子金融活動方法であって、

第１の相互作用可能な安全なノードからの金融情報を有するデジタルコンテナを第２の相互作用可能な安全なノードに通信させる工程と、

モジュラ標準制御情報を該第２の安全なノードに通信させ、該金融情報の少なくとも一部を使用するための条件を少なくとも部分的に設定する工程と、

該使用に関連する情報を該第１の相互作用可能な安全なノードに報告する工程と、

によって特徴づけられる方法。

238．電子金融活動のためのシステムであって、

第１の相互作用可能な安全なノードからの金融情報を有するデジタルコンテナを第２の相互作用可能な安全なノードに通信させる手段と、

モジュラ標準制御情報を該第２の安全なノードに通信させる手段と、

該金融情報の少なくとも一部を使用するための条件を少なくとも部分的に設定する該第２のノードにおける手段と、

該第２の安全なノードからの該使用に関連する情報を該第１の相互作用可能な

安全なノードに報告する手段と、

によって特徴づけられるシステム。

239. 電子通貨管理方法であって、

第１の相互作用可能な安全なユーザノードからの暗号化された電子通貨を、少なくとも１つの安全なコンテナを用いて第２の相互作用可能なユーザノードに通信させる工程と、

該少なくとも１つの安全なコンテナと共に用いられる安全な制御情報であって、条件によって匿名の通貨使用情報を少なくとも部分的に維持する制御情報を提供する工程と、

を包含する方法。

240. 電子通貨管理システムであって、

第１の相互作用可能な安全なユーザノードからの暗号化された電子通貨を、少なくとも１つの安全なコンテナを用いて第２の相互作用可能なユーザノードに通信させる手段と、

該少なくとも１つの安全なコンテナと共に用いられる安全な制御情報であって、条件によって匿名の通貨使用情報を少なくとも部分的に維持する制御情報を提供する手段と、

を有するシステム。

241. 電子金融活動管理方法であって、

金融値チェーンにおいて使用される金融情報の使用を制御するための金融情報標準化制御情報を第１の安全なノードから第２の安全なノードに安全に通信させる工程と、

金融値チェーンにおいて使用される金融情報の使用を制御するための該金融情報標準化制御情報を該第１の安全なノードから第３の安全なノードに安全に通信させる工程と、

安全な制御情報を通信させる工程を包含する、該第２の安全なノードからの暗号化された金融情報を該第３の安全なノードに安全に通信させる工程と、

該第１および第２の安全なノードによって供給される安全な制御情報を少なく

とも部分的に用いて該第３のノードにおいて該金融情報を処理する工程とを包含し、

該標準化制御情報が、該第３の安全なノードに含まれる安全なデータベースに少なくとも部分的に格納される方法。

242. 電子金融活動管理システムであって、

第１および第２の安全なノードと連結される、金融値チェーンにおいて使用される金融情報の使用を制御するための金融情報標準化制御情報を該第１の安全なノードから該第２の安全なノードに安全に通信させる手段と、

該第１の安全なノードと第３のノードとの間で連結される、金融値チェーンにおいて使用される金融情報の使用を制御するための該金融情報標準化制御情報を該第１の安全なノードから該第３の安全なノードに安全に通信させる手段と、

該第２および第３のノード間で連結される、安全な制御情報を通信させることを含む、該第２の安全なノードからの暗号化された金融情報を該第３の安全なノードに安全に通信させる手段と、

該第１および第２の安全なノードによって供給される安全な制御情報を少なくとも部分的に用いて該第３のノードにおいて該金融情報を処理する該第３のノードにおける手段と、

該標準化制御情報を少なくとも部分的に格納する該第３のノードにおける安全なデータベースと、

によって特徴づけられるシステム。

243. 情報管理方法であって、第１のロケーションにおいて少なくとも１つのスマートオブジェクトを作成する工程と、該スマートオブジェクトに割り当てられた少なくとも１つの規則および／または制御を保護する工程を包含する該スマートオブジェクトの少なくとも一部を保護する工程と、該少なくとも１つのスマートオブジェクトを少なくとも１つの第２のロケーションに配布する工程と、該スマートオブジェクトに割り当てられた少なくとも１つの該規則および／または制御の少なくとも一部に従って該少なくとも１つの第２のロケーションにおいて該少なくとも１つのスマートオブジェクトのコンテンツの少なくとも一部を安全に

処理する工程とによって特徴づけられる方法。

244. 情報管理システムであって、

第１のロケーションにおいて少なくとも１つのスマートオブジェクトを作成する手段と、

該スマートオブジェクトに割り当てられた少なくとも１つの規則および／または制御を保護する手段を有する該スマートオブジェクトの少なくとも一部を保護する手段と、

該少なくとも１つのスマートオブジェクトを少なくとも１つの第２のロケーションに配布する手段と、

該スマートオブジェクトに割り当てられた少なくとも１つの該規則および／または制御の少なくとも一部に従って該少なくとも１つの第２のロケーションにおいて該少なくとも１つのスマートオブジェクトのコンテンツの少なくとも一部を安全に処理する手段と、

によって特徴づけられるシステム。

245. オブジェクト処理システムであって、少なくとも部分的に保護された実行可能なコンテンツおよび該コンテンツの実行に関連する動作と関連づけられた少なくとも１つの少なくとも部分的に保護された規則および／または制御を有する少なくとも１つの安全なオブジェクトと、該少なくとも１つの関連づけられた規則および／または制御の少なくとも１つの少なくとも一部に応じて該実行可能なコンテンツを処理する少なくとも１つの安全な実行環境とを有するシステム。

246. オブジェクト処理方法であって、

少なくとも部分的に保護された実行可能なコンテンツおよび該コンテンツの実行に関連する動作と関連づけられた少なくとも１つの少なくとも部分的に保護された規則および／または制御を有する少なくとも１つの安全なオブジェクトを提供する工程と、

該少なくとも１つの関連づけられた規則および／または制御の少なくとも１つの少なくとも一部に応じて該実行可能なコンテンツを少なくとも１つの安全な実行環境内で処理する工程と、

を包含する方法。

247. 権利が配布されたデータベース環境であって、

（ａ）１つまたはそれ以上の中央機関に暗号化されたデジタル情報を使用するための制御情報を確立させる手段と、（ｂ）制御情報および監査情報を安全に格納する複数のユーザサイトにおける相互作用可能なデータベース管理システムと、（ｃ）制御情報および監査情報をユーザサイト間で安全に通信させる安全な通信手段と、（ｄ）複数のユーザサイトからの使用情報を編集および分析する中央データベース手段とを有するデータベース環境。

248. 権利が配布されたデータベース環境において、以下の工程によって特徴づけられる方法であって、

暗号化されたデジタル情報を使用するための制御情報を確立する工程と、

複数のユーザサイトにおける相互作用可能なデータベース管理システム内に制御情報および監査情報を安全に格納する工程と、

制御情報および監査情報をユーザサイト間で安全に通信させる工程と、

複数のユーザサイトからの使用情報を編集および分析する工程と、

によって特徴づけられる方法。

249. 配布されたデータベースをサーチする方法であって、サーチ基準を含む少なくとも１つの安全なオブジェクトを作成する工程と、少なくとも１つの該安全なオブジェクトを少なくとも１つの規則および／または制御に従って１つまたはそれ以上の第２のロケーションに送信してデータベースサーチを実施する工程と、該少なくとも１つの関連づけられた規則および／または制御の少なくとも１つの少なくとも一部に応じて安全なオブジェクト内の該サーチ基準に少なくとも部分的に基づいて少なくとも１つのデータベースサーチを処理する工程と、同一のおよび／または１つもしくはそれ以上の新しい安全なオブジェクト内にデータベースサーチ結果を格納する工程と、サーチ結果を含む該安全なオブジェクトを該第１のロケーションに送信する工程とによって特徴づけられる方法。

250. 前記サーチ結果の少なくとも一部の使用に関連する少なくとも１つの条件

を確立させるための少なくとも１つの他の規則および／または制御と、該サーチ結果とを関連づけるさらなる工程によってさらに特徴づけられる、請求項247に記載の方法。

251．配布されたデータベースをサーチするシステムであって、

サーチ基準を含む少なくとも１つの安全なオブジェクトを作成する手段と、

少なくとも１つの該安全なオブジェクトを少なくとも１つの規則および／または制御に従って１つまたはそれ以上の第２のロケーションに送信してデータベースサーチを実施する手段と、

該少なくとも１つの関連づけられた規則および／または制御の少なくとも１つの少なくとも一部に応じて安全なオブジェクト内の該サーチ基準に少なくとも部分的に基づいて少なくとも１つのデータベースサーチを処理する手段と、

同一のおよび／または１つもしくはそれ以上の新しい安全なオブジェクト内にデータベースサーチ結果を格納する手段と、

サーチ結果を含む該安全なオブジェクトを該第１のロケーションに送信する手段と、

によって特徴づけられるシステム。

252．前記サーチ結果の少なくとも一部の使用に関連する少なくとも１つの条件を確立させるための少なくとも１つの他の規則および／または制御と、該サーチ結果とを関連づける手段によってさらに特徴づけられる、請求項249に記載のシステム。

253．権利管理システムであって、保護された情報と、少なくとも２つの保護された処理配置と、許可された動作および該動作を該保護された処理配置の少なくとも１つによって少なくとも部分的に処理される情報の少なくとも一部に対して実施した結果の表現を可能にする権利管理言語とを有するシステム。

254．権利管理方法であって、

少なくとも２つの保護された処理配置によって処理される保護された情報を提供する工程と、

許可された動作および該動作を該保護された処理配置の少なくとも１つによっ

て少なくとも部分的に処理される該情報の少なくとも一部に対して実施した結果を権利管理言語によって表現する工程と、

を包含する方法。

255. デジタル情報を保護する方法であって、該情報の使用に関連する条件を記述する権利管理言語を用いて該情報の少なくとも一部を暗号化する工程と、該情報の少なくとも一部および該権利言語で表現された条件の少なくとも一部を１つまたはそれ以上の受け手に配布する工程と、少なくとも１つの保護された処理配置を含む電子機器配置を用いて該情報の使用の少なくとも一部を安全に管理する工程とによって特徴づけられる方法。

256. デジタル情報を保護するシステムであって、

該情報の少なくとも一部を暗号化する手段と、

権利管理言語を用いて該情報の使用に関連する条件を記述する手段と、

該情報の少なくとも一部および該権利言語で表現された条件の少なくとも一部を１つまたはそれ以上の受け手に配布する手段と、

該情報の使用の少なくとも一部を安全に管理する少なくとも１つの保護された処理配置を含む電子機器配置と、

によって特徴づけられるシステム。

257. 分散されたデジタル情報管理システムであって、ソフトウェア構成要素と、該ソフトウェア構成要素の２つまたはそれ以上の間の処理関係を表現するための権利管理言語と、該ソフトウェア構成要素の少なくとも一部および該権利管理表現の少なくとも一部の保護された処理手段と、コンテンツを保護する手段と、保護されたコンテンツを該権利管理表現に関連させるソフトウェアオブジェクトを作成する手段と、該保護されたコンテンツ、該権利管理表現、および該ソフトウ

ェアオブジェクトを提供ロケーションからユーザのロケーションに配送する手段とを有するシステム。

258. 分散されたデジタル情報管理方法であって、

ソフトウェア構成要素の２つまたはそれ以上の間の処理関係を権利管理言語で

表現する工程と、

該ソフトウェア構成要素の少なくとも一部および該権利管理表現の少なくとも一部を少なくとも１つの保護された環境において処理する工程と、

コンテンツを保護する工程と、

保護されたコンテンツを該権利管理表現に関連させるソフトウェアオブジェクトを作成する工程と、

該保護されたコンテンツ、該権利管理表現、および該ソフトウェアオブジェクトを提供ロケーションからユーザのロケーションに配送する工程と、

を包含する方法。

259. 認証システムであって、少なくとも２つの電子機器と、異なる証明秘密鍵を用いて暗号化されたID情報を反映する少なくとも２つのデジタル証明書であって、該証明書が第１の電子機器に格納される証明書と、電子機器間で信号を送信および受信する通信手段と、第２の電子機器に操作によって接続される侵犯されたおよび／または満期になった証明秘密鍵を決定する手段と、該第２の電子機器が、該決定に少なくとも部分的に基づいて該第１の電子機器からの該デジタル証明書の１つの送信をリクエストする手段と、該第２の電子機器に操作によって接続される、該証明書を復号化し、該証明書の有効性および／または該ID情報の有効性を決定する手段とを有するシステム。

260. 少なくとも２つの電子機器を有するシステムにおいて、

ID情報を反映する少なくとも２つのデジタル証明書を発行する工程であって、異なる証明秘密鍵を用いて該２つの証明書を暗号化する工程を包含する工程と、

該証明書を第１の電子機器に格納する工程と、

電子機器間で信号を送信および受信する工程と、

第２の電子機器に操作によって接続される侵犯されたおよび／または満期になった証明秘密鍵を決定する工程と、

該第２の電子機器を用いて、該決定に少なくとも部分的に基づいて該第１の電子機器からの該デジタル証明書の１つの送信をリクエストする工程と、

該第２の電子機器を用いて該証明書を復号化する工程と、

該証明書の有効性および／または該ID情報の有効性を決定する工程と、

を包含する認証方法。

261. 認証システムであって、少なくとも２つの電子機器と、異なる証明秘密鍵を用いて暗号化されたID情報を反映する少なくとも２つのデジタル証明書であって、該証明書が第１の電子機器に格納される証明書と、電子機器間で信号を送信および受信する通信手段と、第２の電子機器が、該第１の電子機器からの該デジタル証明書の１つの送信をリクエストする手段であって、該証明書の選択が乱数または擬乱数に少なくとも部分的に基づいてリクエストされる手段と、該第２の電子機器に操作によって接続される、該証明書を復号化し、該証明書の有効性および／またはID情報の有効性を決定する手段とを有するシステム。

262. 少なくとも２つの電子機器を有するシステムにおいて、

ID情報を反映する少なくとも２つのデジタル証明書を発行する工程であって、異なる証明秘密鍵を用いて該２つの証明書を暗号化する工程を包含する工程と、

該証明書を第１の電子機器に格納する工程と、

電子機器間で信号を送信および受信する工程と、

第２の電子機器を用いて、該第１の電子機器からの該デジタル証明書の１つの送信をリクエストする工程であって、乱数または擬乱数に少なくとも部分的に基づいて証明書を選択する工程を包含する工程と、

該第２の電子機器を用いて該証明書を復号化する工程と、

該証明書の有効性および／または該ID情報の有効性を決定する工程と、

を包含する認証方法。

263. 安全な電子メールの方法であって、相互作用可能な保護された処理環境を用いて少なくとも１つの電子メッセージを作成する工程と、該少なくとも１つのメッセージの少なくとも一部を暗号化する工程と、１つまたはそれ以上のセットの制御情報と、１つまたはそれ以上のメッセージとを安全に関連づけ、該少なくとも１つのメッセージを使用するための少なくとも１つの条件を設定する工程と、該保護された電子メッセージを該保護された処理環境を有する１つまたはそれ以上の受け手に通信させる工程と、同一または異なる制御情報の少なくとも１つ

のセットを各受け手に安全に通信させる工程と、制御情報および保護されたメッセージの両方の受け手が該制御情報によって指定される条件に少なくとも部分的に従ってメッセージ情報を用いることを可能にする工程とによって特徴づけられる方法。

264．多数の保護された処理環境を有する安全な電子メールのためのシステムであって、

少なくとも１つの電子メッセージを作成する第１の保護された処理環境であって、該少なくとも１つのメッセージの少なくとも一部を暗号化する手段と、１つまたはそれ以上のセットの制御情報と、１つまたはそれ以上のメッセージとを安全に関連づけ、該少なくとも１つのメッセージを使用するための少なくとも１つの条件を設定する手段と、該保護された電子メッセージを相互作用可能な保護された処理環境を有する１つまたはそれ以上の受け手に通信させる手段とを有する処理環境と、

同一または異なる制御情報の少なくとも１つのセットを各受け手に安全に通信させる手段と、

制御情報および保護されたメッセージの両方の受け手が該制御情報によって指定される条件に少なくとも部分的に従ってメッセージ情報を用いることを可能にする手段とによって特徴づけられるシステム。

265．情報管理方法であって、不許可使用からコンテンツを保護する工程と、使用可能制御情報と該保護されたコンテンツの少なくとも一部とを安全に関連づける工程であって、該使用可能制御情報が、該使用可能制御情報がどのように再配布され得るかを記述する情報を導入する工程と、該保護されたコンテンツの少なくとも一部を第１のユーザに配送する工程と、該使用可能制御情報を該第１のユーザに配送する工程と、該使用可能制御情報を再配布するためのリクエストを該第１のユーザから受け取る工程と、該使用可能制御情報がどのように再配布され得るかの記述を用いて新しい使用可能制御情報を作成する工程であって、該新しい使用可能制御情報が該第１のユーザによって受け取られる該使用可能制御情報と同一または異なり得る工程と、該新しい使用可能制御情報および／または保護

された情報を第２のユーザに配送する工程とによって特徴づけられる方法。

２６６．情報管理システムであって、

不許可使用からコンテンツを保護する手段と、

使用可能制御情報と、該保護されたコンテンツの少なくとも一部とを安全に関連づける手段であって、該使用可能制御情報がどのように再配布され得るかを記述する使用可能制御情報を導入する手段を有する手段と、

該保護されたコンテンツの少なくとも一部を第１のユーザに配送する手段と、

該使用可能制御情報を該第１のユーザに配送する手段と、

該使用可能制御情報を再配布するためのリクエストを該第１のユーザから受け取る手段と、

該使用可能制御情報がどのように再配布され得るかの記述を用いて新しい使用可能制御情報を作成する手段であって、該新しい使用可能制御情報が該第１のユーザによって受け取られる該使用可能制御情報と同一または異なり得る手段と、

該新しい使用可能制御情報および／または保護された情報を第２のユーザに配送する手段とによって特徴づけられるシステム。

２６７．配布されたデジタル情報の再配布を制御する方法であって、デジタル情報を暗号化する工程と、該暗号化されたデジタル情報を第１のパーティから第２のパーティに再配布する工程と、該第２のパーティから少なくとも１つの第３のパーティへの該暗号化されたデジタル情報の少なくとも一部の再配布に関する制御情報を確立する工程と、該制御情報を処理する保護された処理環境を用いて該暗号化されたデジタル情報の該少なくとも一部の再配布を制御する工程とを包含する方法。

２６８．配布されたデジタル情報の再配布を制御するシステムであって、

デジタル情報を暗号化する手段と、

該暗号化されたデジタル情報を第１のパーティから少なくとも１つの第２のパーティに再配布する手段と、

該第２のパーティから少なくとも１つの第３のパーティへの該暗号化されたデジタル情報の少なくとも一部の再配布に関する制御情報を確立する手段と、

該制御情報を処理し、該暗号化されたデジタル情報の該少なくとも一部の再配布を制御する保護された処理環境と、

を有するシステム。

269. ロボットを制御する方法であって、１つまたはそれ以上のロボット用の命令を作成する工程と、該命令を組み入れる安全なコンテナを作成する工程と、制御情報と該安全なコンテナとを関連づける工程と、少なくとも１つの安全な処理ユニットを該１つまたはそれ以上のロボットに組み入れる工程と、該制御情報の少なくとも一部に従って該命令の少なくとも一部を実施する工程とによって特徴づけられる方法。

270. 前記制御情報が、前記命令が使用され得る条件および該命令が実施されるときに要求される監査レポートの特性を記述する情報を有することによってさらに特徴づけられる、請求項267に記載の方法。

271. ロボット制御システムであって、

１つまたはそれ以上のロボット用の命令を作成する手段と、

該命令を導入する安全なコンテナを作成する手段と、

制御情報と該安全なコンテナとを関連づける手段と、

少なくとも１つの安全な処理ユニットを該１つまたはそれ以上のロボットに組み入れる手段と、

該制御情報の少なくとも一部に従って該命令の少なくとも一部を実施する手段と、

によって特徴づけられるシステム。

272. 前記命令が使用され得る条件および該命令が実施されるときに要求される監査レポートの特性を記述する手段を有する前記制御情報を作成する手段によってさらに特徴づけられる、請求項269に記載のシステム。

273. 電子商取引における詐欺を検出する方法であって、少なくとも１つの安全なコンテナを作成する工程と、制御情報と、監査情報が収集され監査パーティに送信されることを要求する制御情報を含む該１つまたはそれ以上のコンテナとを関連づける工程と、該１つまたはそれ以上のコンテナおよび該制御情報を少なく

とも１つのユーザに配送する工程と、各コンテナおよび該各ユーザを同定する情報を記録する工程と、監査情報を受け取る工程と、該受け取れらた監査情報および／または該制御情報に少なくとも部分的に基づいて使用のプロファイルを作成する工程と、特定の監査情報が該使用のプロファイルと少なくとも部分的に異なる場合を検出する工程とによって特徴づけられる方法。

274．電子商取引における詐欺を検出するシステムであって、

少なくとも１つの安全なコンンテナを作成する手段と、

制御情報と、監査情報が収集され監査パーティに送信されることを要求する制御情報を含む該１つまたはそれ以上のコンテナとを関連づける手段と、

該１つまたはそれ以上のコンテナおよび該制御情報を少なくとも１つのユーザに配送する手段と、

各コンテナおよび該各ユーザを同定する情報を記録する手段と、

監査情報を受け取る手段と、

該受け取った監査情報および／または該制御情報に少なくとも部分的に基づいて使用のプロファイルを作成する手段と、

特定の監査情報が該使用のプロファイルと少なくとも部分的に異なる場合を検出する手段と、

によって特徴づけられるシステム。

275．電子商取引における詐欺を検出する方法であって、少なくとも部分的に保護されたデジタル情報をカスタマに配布する工程と、該デジタル情報の少なくとも一部を電子ネットワークにわたって使用するための１つまたはそれ以上の権利を配布する工程と、保護された処理環境および該１つまたはそれ以上の配布された権利の少なくとも１つを用いて該少なくとも部分的に保護されたデジタル情報の少なくとも一部をカスタマに使用させる工程と、該デジタル情報の使用に関連する異常な使用活動を検出する工程とによって特徴づけられる方法。

276．電子商取引における詐欺を検出するシステムであって、

少なくとも部分的に保護されたデジタル情報をカスタマに配布する手段と、

該デジタル情報の少なくとも一部を電子ネットワークにわたって使用するため

の１つまたはそれ以上の権利を配布する手段と、

該１つまたはそれ以上の配布された権利の少なくとも１つを通じて該少なくとも部分的に保護されたデジタル情報の少なくとも一部をカスタマに使用させる保護された処理環境と、

該デジタル情報の使用に関連する異常な使用活動を検出する手段と、

によって特徴づけられるシステム。

277. プログラム可能な構成要素配置であって、マイクロプロセッサ、メモリ、タスクマネージャー、メモリマネージャーおよび外部インターフェースコントローラを有する不正改変不可能な処理環境と、任意の構成要素を少なくとも部分的に該メモリにロードする手段と、該構成要素の処理に関連づけられた１つまたはそれ以上のタスクを初期化する手段と、該構成要素の有効性、完全性および／または信頼性を証明する手段と、任意の構成要素を作成する手段と、任意のイベントと該作成された構成要素とを関連づける手段と、該作成された構成要素の有効性、完全性および／または信頼性を証明する手段と、該作成された構成要素を安全に配送する手段とを有する配置。

278. マイクロプロセッサ、メモリ、タスクマネージャー、メモリマネージャーおよび外部インターフェースコントローラを備えた不正改変不可能な処理環境を有するプログラム可能な構成要素配置において、以下の工程によって特徴づけられる方法であって、

任意の構成要素を作成する工程と、

任意のイベントと該作成された構成要素とを関連づける工程と、

該任意の構成要素を少なくとも部分的に該メモリにロードする工程と、

該ロードされた構成要素の処理に関連づけられた１つまたはそれ以上のタスクを初期化する工程と、

該作成された構成要素の有効性、完全性および／または信頼性を証明する工程と、

該作成された構成要素を安全に配送する工程と、

によって特徴づけられる方法。

279. 配布された保護されたプログラム可能な構成要素配置であって、マイクロプロセッサ、メモリ、タスクマネージャー、メモリマネージャーおよび外部インターフェースコントローラを有する少なくとも２つの不正改変不可能な処理環境と、任意の構成要素を少なくとも部分的に該メモリにロードする手段と、該構成要素の処理に関連づけられた１つまたはそれ以上のタスクを初期化する手段と、該構成要素の有効性、完全性および／または信頼性を証明する手段とを有し、任意の構成要素を作成する手段と、任意のイベントと該作成された構成要素とを関連づける手段と、該作成された構成要素の有効性、完全性および／または信頼性を証明する手段と、該作成された構成要素を該少なくとも２つの不正改変不可能な処理環境の少なくとも２つの間で安全に配送する手段とをさらに有する配置。

280. マイクロプロセッサ、メモリ、タスクマネージャー、メモリマネージャーおよび外部インターフェースコントローラを有する少なくとも２つの不正改変不可能な処理環境を有する配布された保護されたプログラム可能な構成要素配置において、

任意の構成要素を作成する工程と、

該構成要素の有効性、完全性および／または信頼性を証明する工程と、

該任意の構成要素を少なくとも部分的に該メモリにロードする工程と、

該構成要素の処理に関連づけられた１つまたはそれ以上のタスクを初期化する工程と、

任意のイベントと該作成された構成要素とを関連づける工程と、

該作成された構成要素を該少なくとも２つの不正改変不可能な処理環境の少なくとも２つの間で安全に配送する工程と、

を有する方法。

281. 少なくとも１つのCPUと、メモリと、少なくとも１つのシステムバスと、少なくとも１つの保護された処理環境と、ホスト動作システムに関連づけられた権利オペレーティングシステムまたは権利オペレーティングシステム層の少なくとも１つとを有する電子機器。

282. 少なくとも１つのタスクマネージャーと、少なくとも１つのメモリマネー

ジャーと、少なくとも１つの入力／出力マネージャーと、少なくとも１つの保護された処理環境と、イベントを検出する手段と、イベントと権利制御機能とを関連づける手段と、該１つまたはそれ以上の保護された処理環境内で少なくとも部分的に権利制御機能を実施する手段とを有するオペレーティングシステム。

283．少なくとも１つのタスクマネージャーと、少なくとも１つのメモリマネージャーと、少なくとも１つの入力／出力マネージャーと、少なくとも１つの保護された処理環境とを有するオペレーティングシステムにおいて、

イベントを検出する工程と、

該イベントと権利制御機能とを関連づける工程と、

該１つまたはそれ以上の保護された処理環境内で少なくとも部分的に権利制御機能を実施する工程と、

を包含する方法。

284．ビジネス自動化方法であって、決算および／または管理情報を含む１つまたはそれ以上の安全なコンテナを作成する工程と、（ａ）該コンテナが配送され得るおよび／または配送されなければならない１つまたはそれ以上のパーティ、および／または（ｂ）該決算および／または他の管理情報に関して該１つまたはそれ以上のパーティが成し遂げ得るおよび／または成し遂げなければならない動作の記述を含む制御情報と、該１つまたはそれ以上の安全なコンテナとを関連づける工程と、該コンテナを該１つまたはそれ以上のパーティに配送する工程と、該１つまたはそれ以上のパーティによる該決算および／または他の管理情報の使用前、使用中および／または使用後に該制御情報の少なくとも一部の記述および／または実施を有効にする工程とによって特徴づけられる方法。

285．前記制御情報が、監査情報が収集され１つまたはそれ以上の監査パーティに配送されるという少なくとも１つの要件をさらに有し、該監査情報の少なくとも一部を１つまたはそれ以上のパーティに配送する工程をさらに包含する、請求項282に記載の方法。

286．前記監査情報の少なくとも一部が、前記監査パーティの少なくとも１つによって自動的に処理され、さらなる決算、管理および／または監査情報を、監査

情報を送信した前記１つまたはそれ以上のパーティと同一および／または異なり得る１つまたはそれ以上のパーティに、該受信された監査情報の受信および／またはコンテンツに少なくとも部分的に基づいて送信する工程をさらに包含する、請求項283に記載の方法。

287. 前記パーティの少なくとも２つが、異なるビジネスおよびまたは他の組織と関連づけられ、前記制御情報が、該ビジネスおよび／または他の組織間の決算、管理、報告および／または他の監査関係を少なくとも部分的に記述する情報を含む、請求項282に記載の方法。

288. 前記決算および／または他の管理情報のいくらかまたはすべてが前記制御情報に含まれる、請求項282、283，284または285に記載の方法。

289. ビジネス自動化システムであって、

決算および／または他の管理情報を含む１つまたはそれ以上の安全なコンテナを作成する手段と、

（ａ）該コンテナが配送され得るおよび／または配送されなければならない１つまたはそれ以上のパーティ、および／または（ｂ）該決算および／または他の管理情報に関して該１つまたはそれ以上のパーティが成し遂げ得るおよび／または成し遂げなければならない動作の記述を含む制御情報と、該１つまたはそれ以上の安全なコンテナとを関連づける手段と、

該コンテナの１つまたはそれ以上を１つまたはそれ以上のパーティに配送する手段と、

該１つまたはそれ以上のパーティによる該決算および／または他の管理情報の使用前、使用中および／または使用後に該制御情報の少なくとも一部の記述および／または実施を有効にする手段と、

によって特徴づけられるシステム。

290. 前記関連づけ手段が、監査情報が収集され１つまたはそれ以上の監査パーティに配送されるという少なくとも１つの要件を関連づける手段をさらに有し、前記配送手段が、該監査情報の少なくとも一部を１つまたはそれ以上のパーティに配送する手段を有する、請求項287に記載のシステム。

291. 前記監査情報の少なくとも一部を自動的に処理する手段をさらに有し、さらなる決算、管理および／または監査情報を、監査情報を送信した前記１つまたはそれ以上のパーティと同一および／または異なり得る１つまたはそれ以上のパーティに、該受信された監査情報の受信および／またはコンテンツに少なくとも部分的に基づいて送信する手段をさらに有する、請求項288に記載のシステム。

292. 前記パーティの少なくとも２つが、異なるビジネスおよびまたは他の組織と関連づけられ、前記関連づけ手段が、該ビジネスおよび／または他の組織間の決算、管理、報告および／または他の監査関係を少なくとも部分的に記述する情報を含む制御情報を生成する手段を有する、請求項287に記載の方法。

293. 前記決算および／または他の管理情報のいくらかまたはすべてが前記制御情報に含まれる、請求項286、287、288または290に記載のシステム。

294. コンテンツを配布する方法であって、１つまたはそれ以上の第１の安全なコンテナを作成する工程と、該第１のコンテナのコンテンツのいくらかまたはすべてが抽出され得る条件を記述する情報を含む制御情報と、該第１のコンテナとを関連づける工程と、該第１のコンテナの少なくとも一部および該制御情報を１つまたはそれ以上のパーティに配送する工程と、該パーティの１つまたはそれ以上によるリクエストを検出して該第１のコンテナの該コンテンツのいくらかまたはすべてを抽出する工程と、該リクエストおよび該制御情報に従って１つまたはそれ以上の第２の安全なコンテナを作成する該制御情報によって許可される程度に、該リクエストが該制御情報によって全体的または部分的に許可されるかどうかを決定する工程と、該第１のコンテナと関連づけられた該制御情報に少なくとも部分的に基づいて該制御情報と該１つまたはそれ以上の第２の安全なコンテナとを関連づける工程とによって特徴づけられる方法。

295. コンテンツを配布するシステムであって、

１つまたはそれ以上の第１の安全なコンテナを作成する手段と、

該第１のコンテナのコンテンツのいくらかまたはすべてが抽出され得る条件を記述する情報を含む制御情報と、該第１のコンテナとを関連づける手段と、

該第１のコンテナの少なくとも一部および該制御情報を１つまたはそれ以上のパーティに配送する手段と、

該パーティの１つまたはそれ以上によるリクエストを検出して該第１のコンテナの該コンテンツのいくらかまたはすべてを抽出する手段と、

該リクエストおよび該制御情報に従って１つまたはそれ以上の第２の安全なコンテナを作成する該制御情報によって許可される程度に、該リクエストが該制御情報によって全体的または部分的に許可されるかどうかを決定する手段と、

該第１のコンテナと関連づけられた該制御情報に少なくとも部分的に基づいて該制御情報と該１つまたはそれ以上の第２の安全なコンテナとを関連づける手段と、

によって特徴づけられるシステム。

296．コンテンツを配布する方法であって、１つまたはそれ以上の第１の安全なコンテナを作成する工程と、該第１のコンテナが（ａ）１つまたはそれ以上の第２の安全なコンテナに全体的または部分的に埋め込まれおよび／または安全に関連づけられ得る、および／または（ｂ）１つまたはそれ以上の安全なコンテナを該第１の安全なコンテナに全体的または部分的に埋め込ませるおよび／または安全に関連づけさせ得る条件を記述する情報を含む制御情報と、該第１の安全なコンテナとを関連づける工程と、該第１の安全なコンテナの少なくとも一部および該制御情報を１つまたはそれ以上のパーティに配送する工程と、該パーティの１つまたはそれ以上あるいは他のパーティによるリクエストを検出して、該１つまたはそれ以上の第２のコンテナを全体的または部分的に該第１のコンテナに埋め込むおよび／または安全に関連づける、および／または（ｂ）該第１の安全なコンテナを全体的または部分的に安全なコンテナに埋め込むおよび／または安全に関連づける工程と、１つまたはそれ以上の埋め込みおよび／または安全な関連づけ動作を行う制御情報によって許可される程度、ならびに制御情報によって要求されおよび／または該パーティの１つまたはそれ以上によってリクエストされる程度に、該リクエストが制御情報によって許可されるかどうかを決定する工程と、少なくとも部分的に該１つまたはそれ以上の埋め込みおよび／または安全な関連

づけ動作の結果として、新しい制御情報を改変および／または作成する工程とによって特徴づけられる方法。

297. コンテンツを配布するシステムであって、

１つまたはそれ以上の第１の安全なコンテナを作成する手段と、

該第１の安全なコンテナが（ａ）１つまたはそれ以上の第２の安全なコンテナに全体的または部分的に埋め込まれおよび／または安全に関連づけられ得る、および／または（ｂ）１つまたはそれ以上の安全なコンテナを該第１の安全なコンテナに全体的または部分的に埋め込ませるおよび／または安全に関連づけさせ得る条件を記述する情報を含む制御情報と、該第１の安全なコンテナとを関連づける手段と、

該第１の安全なコンテナの少なくとも一部および該制御情報を１つまたはそれ以上のパーティに配送する手段と、

該パーティの１つまたはそれ以上によるリクエストを検出して、該１つまたはそれ以上の第２のコンテナを全体的または部分的に該第１のコンテナに埋め込むおよび／または安全に関連づける、および／または（ｂ）該第１の安全なコンテナを全体的または部分的に安全なコンテナに埋め込むおよび／または安全に関連づける手段と、

１つまたはそれ以上の埋め込みおよび／または安全な関連づけ動作を実施する制御情報によって許可される程度、ならびに制御情報によって要求されおよび／または該パーティの１つまたはそれ以上によってリクエストされる程度に、該リクエストが制御情報によって許可されるかどうかを決定し、少なくとも部分的に該１つまたはそれ以上の埋め込みおよび／または安全な関連づけ動作の結果として、新しい制御情報を改変および／または作成する手段と、

によって特徴づけられるシステム。

298. 情報を配布する方法であって、不許可使用から情報を保護する工程と、制御情報と該保護された情報とを関連づける工程と、複数の通路を用いて該保護された情報の少なくとも一部を１つまたはそれ以上のパーティに配送する工程と、

同一または異なる複数の通路を用いて該制御情報の少なくとも一部を１つまたは

それ以上のパーティに配送する工程と、少なくとも一部が第２の通路を用いて配送される制御情報に従って、該パーティの少なくとも１つが、第１の通路を用いて配送された該保護された情報を少なくともいくらかを利用できるようにする工程とによって特徴づけられる方法。

299．保護された情報および／または制御情報を配送する該通路の少なくとも１つが該制御情報によって記述される、請求項296に記載の方法。

300．情報を配布するシステムであって、

不許可使用から情報を保護する手段と、

制御情報と該保護された情報とを関連づける手段と、

複数の通路を用いて該保護された情報の少なくとも一部を１つまたはそれ以上のパーティに配送する手段と、

同一または異なる複数の通路を用いて該制御情報の少なくとも一部を１つまたはそれ以上のパーティに配送する手段と、

少なくとも一部が第２の通路を用いて配送される制御情報に従って、該パーティの少なくとも１つが、第１の通路を用いて配送された該保護された情報を少なくともいくらかを利用できるようにする手段と、

によって特徴づけられるシステム。

301．前記配送手段が、前記制御情報によって記述される保護された情報および／または制御情報を前記通路の少なくとも１つにわたって配送する手段を有する、請求項298に記載のシステム。

302．情報を配布する方法であって、不許可使用から情報を保護する工程と、監査情報の収集を要求する情報を含む制御情報と該保護された情報とを関連づける工程と、１つまたはそれ以上のパーティが監査情報を受信および／または処理することを可能にする工程と、該保護された情報の少なくとも一部および該制御情報を１つまたはそれ以上のパーティに配送する工程と、該監査情報の収集を要求する該制御情報の少なくとも一部に従って該保護された情報の少なくともいくらかの使用を有効にする工程と、該配送パーティとは異なる該有効となった監査パーティの１つまたはそれ以上に該監査情報を配送する工程とによって特徴づけら

れる方法。

303. 前記監査パーティの少なくとも１つが、前記制御情報において指定される、請求項300に記載の方法。

304. 情報を配布するシステムであって、

不許可使用から情報を保護する手段と、

監査情報の収集を要求する情報を含む制御情報と該保護された情報とを関連づける手段と、

１つまたはそれ以上のパーティが監査情報を受信および／または処理することを可能にする手段と、

該保護された情報の少なくとも一部および該制御情報を１つまたはそれ以上のパーティに配送する手段と、

該監査情報の収集を要求する該制御情報の少なくとも一部に従って該保護された情報の少なくともいくらかの使用を有効にする手段と、

該配送パーティとは異なる該有効となった監査パーティの１つまたはそれ以上に該監査情報を配送する手段と、

によって特徴づけられるシステム。

305. 前記監査パーティの少なくとも１つが、前記制御情報において指定される、請求項302に記載のシステム。

306. 安全な構成要素をベースとした動作プロセスであって、

（ａ）少なくとも１つの構成要素を検索する工程と、

（ｂ）構成要素アセンブリを指定する記録を検索する工程と、

（ｃ）該構成要素および／または該記録の有効性をチェックする工程と、

（ｄ）該記録に従って該構成要素を用いて該構成要素アセンブリを形成する工程と、

（ｅ）該構成要素アセンブリに少なくとも部分的に基づいてプロセスを実施する工程と、

を包含するプロセス。

307. 前記工程（ｃ）が前記構成要素アセンブリを実行する工程をさらに包含す

る、請求項304に記載のプロセス。

308. 前記構成要素が実行可能なコードを有する、請求項304に記載のプロセス。

309. 前記構成要素がロードモジュールを有する、請求項304に記載のプロセス。

310. 前記記録が、

（ｉ）前記構成要素アセンブリを組み立てる指令と、

（ii）少なくとも部分的に制御を指定する情報とを有し、

該制御に少なくとも部分的に基づいて前記工程（ｄ）および／または前記工程（ｅ）を制御する工程をさらに包含する、請求項304に記載のプロセス。

311. 前記構成要素がセキュリティラッパ(security wrapper)を有し、前記制御工程が、前記制御に少なくとも部分的に基づいて該セキュリティラッパを選択的に開く工程を包含する、請求項304に記載のプロセス。

312. 前記パーミッション記録が、少なくとも１つの復号化鍵を有し、

前記制御工程が、該復号化鍵の使用を制御する工程を包含する、請求項304に記載のプロセス。

313. 保護された処理環境内で前記工程（ａ）および（ｅ）の少なくとも２つを実施する工程を包含する、請求項304に記載のプロセス。

314. 少なくとも部分的に不正改変不可能なハードウェア内で前記工程（ａ）および（ｅ）の少なくとも２つを実施する工程を包含する、請求項304に記載のプロセス。

315. 前記実施する工程（ｅ）が使用を計量する工程を包含する、請求項304に記載の方法。

316. 前記実施する工程（ｅ）が使用を監査する工程を包含する、請求項304に記載の方法。

317. 前記実施する工程（ｅ）が使用の予算を作成する工程を包含する、請求項304に記載の方法。

318. 安全な構成要素動作システムプロセスであって、

構成要素を受け取る工程と、

該構成要素の使用を指定する指令を受け取り構成要素アセンブリを形成する工

程と、

該受け取った構成要素および／または該指令を認証する工程と、

該構成要素を用いて、該受け取った指令に少なくとも部分的に基づいて該構成要素アセンブリを形成する工程と、

該構成要素アセンブリを用いて少なくとも１つの動作を実施する工程と、

を包含するプロセス。

319．安全な動作システム環境内で以下の工程を実施することを含む方法であって、

コードを提供する工程と、

該コードのアセンブリを実行可能なプログラムに指定する指令を提供する工程と、

該受け取ったコードおよび／または該アセンブリのディレクタの有効性をチェックする工程と、

イベントの発生に応答して、該受け取ったアセンブリの指令に従って該コードを組み立て、実行するためのアセンブリを形成する工程と、

を実施することを含む方法。

320．安全な動作環境を用いて少なくとも１つのリソースを管理する方法であって、

該動作環境の外部にある第１のエンティティから第１の制御を安全に受け取る工程と、

該動作環境の外部にある第２のエンティティから第２の制御を安全に受け取る工程であって、該第２のエンティティが該第１のエンティティとは異なる工程と、

少なくとも１つのリソースを用いて、該第１および第２の制御と関連づけられたデータアイテムを安全に処理する工程と、

該第１および第２の制御を安全に適用し、該データアイテムと共に使用される該リソースを管理する工程と、

を包含する方法。

321. 電子配置によって少なくとも部分的に実施されるデータアイテム上での少なくとも１つの動作を安全に管理する方法であって、

（ａ）第１の手続きを該電子配置に安全に配送する工程と、

（ｂ）該第１の手続きと分離可能または分離した第２の手続きを該電子配置に安全に配送する工程と、

（ｃ）該データアイテム上で少なくとも１つの動作を実施する工程であって、該第１および第２の手続きを組み合わせて使用し、該動作を少なくとも部分的に安全に管理する工程を包含する工程と、

（ｄ）発生した該配送工程（ａ）および（ｂ）に基づいて該データアイテムの使用の少なくとも１つの局面を安全に条件づける工程と、

を包含する方法。

322. 前記配送工程（ａ）が実施される時点とは異なる時点で前記配送工程（ｂ）を実施する工程を包含する、請求項319に記載の方法。

323. 前記工程（ａ）が前記第１の手続きを第１のソースから配送する工程を包含し、前記工程（ｂ）が前記第２の手続きを該第１のソースとは異なる第２のソースから配送する工程を包含する、請求項319に記載の方法。

324. 前記第１および第２の手続きの完全性を確実にする工程をさらに包含する、請求項319に記載の方法。

325. 前記第１および第２の手続きのそれぞれの有効性を検査する工程をさらに包含する、請求項319に記載の方法。

326. 前記第１および第２の手続きのそれぞれを認証する工程をさらに包含する、請求項319に記載の方法。

327. 前記使用する工程（ｃ）が、不正改変不可能な環境内で前記第１および第２の手続きの少なくとも１つを実行する工程を包含する、請求項319に記載の方法。

328. 前記工程（ｃ）が、前記データアイテムを前記第１および第２の手続きの少なくとも１つを用いて制御する工程を包含する、請求項319に記載の方法。

329. 前記第１および第２の手続きの少なくとも１つと前記データアイテムとの

間の関係を確立する工程をさらに包含する、請求項319に記載の方法。

330. 前記データアイテムと、前記第１および第２の手続きの少なくとも１つとの間の対応を確立する工程をさらに包含する、請求項319に記載の方法。

331. 前記配送工程（ｂ）が、少なくとも部分的に暗号化された少なくとも１つのロードモジュールを配送する工程を包含する、請求項319に記載の方法。

332. 前記配送工程（ａ）が、少なくとも部分的に暗号化された少なくとも１つの他のロードモジュールを配送する工程を包含する、請求項329に記載の方法。

333. 前記配送工程（ｂ）が、少なくとも部分的に安全な制御情報を搬送する少なくとも１つのコンテンツコンテナを配送する工程を包含する、請求項319に記載の方法。

334. 前記配送工程（ｂ）が、制御メソッドおよび少なくとも１つの他のメソッドを配送する工程を包含する、請求項319に記載の方法。

335. 前記配送工程（ａ）が、

前記第１の手順の少なくとも一部を暗号化する工程と、

前記少なくとも部分的に暗号化された第１の手続きを前記電子配置に通信させる工程と、

該電子配置を少なくとも部分的に用いて該第１の手続きの少なくとも一部を復号化する工程と、

該第１の手続きを該電子配置を用いて有効性を検査する工程と、

を包含する、請求項319に記載の方法。

336. 前記配送工程（ｂ）が、前記第１および第２の手続きを管理オブジェクト内に配送する工程を包含する、請求項319に記載の方法。

337. 前記配送工程（ｂ）が、前記第２の手続きを少なくとも部分的に暗号化された形式で前記データアイテムと共に共配送する工程を包含する、請求項319に記載の方法。

338. 前記実施する工程が使用を計量する工程を包含する、請求項319に記載の方法。

３３９．前記実施する工程が使用を監査する工程を包含する、請求項３１９に記載の方法。

３４０．前記実施する工程が使用の予算を作成する工程を包含する、請求項３１９に記載の方法。

３４１．安全な電子機器によって少なくとも部分的に実施される少なくとも１つの動作を安全に管理する方法であって、

（ａ）少なくとも１つの動作に対して保護されるアイテムを選択する工程と、

（ｂ）複数の分離された手続きを該電子機器に安全に独立して配送する工程と、

（ｃ）該複数の分離された手続きを組み合わせて使用し、該選択されたアイテムに対して該動作を少なくとも部分的に安全に管理する工程と、

（ｄ）発生した該配送工程（ｂ）における該動作の完了の成功を条件づける工程と、

を包含する方法。

３４２．デリバラブル(deliverables)に基づいた処理方法であって、

プロセスの第１の部分を定義するコードの第１のピースを安全に配送する工程と、

該プロセスの第２の部分を定義するコードの第２のピースを個別かつ安全に配送する工程と、

該第１および第２の配送されたコードのピースの完全性を確実にする工程と、

該第１および第２の配送されたコードのピースに少なくとも部分的に基づいて該プロセスを実施する工程と、

を包含する方法。

３４３．前記プロセスのコードの第１のピースが復号化コンテンツを少なくとも部分的に制御する、請求項３４０に記載の方法。

３４４．前記確実にする工程が、前記コードの第１および第２のピースの有効性を検査する工程を包含する、請求項３４０に記載の方法。

３４５．前記確実にする工程が、前記コードの第１および第２のピースを互いに対

して有効性を検査する工程を包含する、請求項340に記載の方法。

346. 前記実施する工程が使用を計量する工程を包含する、請求項340に記載の方法。

347. 前記実施する工程が活動を監査する工程を包含する、請求項340に記載の方法。

348. 前記実施する工程が使用の予算を作成する工程を包含する、請求項340に記載の方法。

349. 前記実施する工程が、電子制御に基づいてコンテンツを電子的に処理する工程を包含する、請求項340に記載の方法。

350. データアイテムに対して少なくとも１つの保護された動作を安全に制御する方法であって、

（ａ）第１のパーティから少なくとも第１の制御を供給する工程と、

（ｂ）該第１のパーティとは異なる第２のパーティから少なくとも第２の制御を供給する工程と、

（ｃ）該第１および第２の制御を安全に組み合わせて制御のセットを形成する工程と、

（ｄ）該制御セットと該データアイテムとを安全に関連づける工程と、

（ｅ）該制御セットに基づいて該データアイテムに対して少なくとも１つの保護された動作を安全に制御する工程と、

を包含する方法。

351. 前記データアイテムが保護されている、請求項348に記載の方法。

352. 前記複数の制御の少なくとも１つが、前記保護されたデータアイテムの使用の少なくとも１つの局面を計量することに関連する制御を有する、請求項348に記載の方法。

353. 前記複数の制御の少なくとも１つが、前記保護されたデータアイテムの使用の少なくとも１つの局面を予算作成することに関連する制御を有する、請求項348に記載の方法。

354. データアイテムを組み合わせて複合データアイテムにする安全な方法であ

って、

（ａ）関連づけられた少なくとも第１の制御を有する第１のデータアイテムを安全に提供する工程と、

（ｂ）関連づけられた少なくとも第２の制御を有する第２のデータアイテムを安全に提供する工程と、

（ｃ）該第１および第２のデータアイテムの複合体を形成する工程と、

（ｄ）該第１および第２の制御を安全に組み合わせて複合制御セットにする工程と、

（ｅ）該複合制御セットに少なくとも部分的に基づいて該第１および第２のデータアイテムの該複合体に対して少なくとも１つの動作を実施する工程と、

を包含する方法。

355．前記組み合わせ工程が、前記第１および第２の制御のそれぞれを前記複合セット内に保存する工程を包含する、請求項352に記載の方法。

356．前記実施する工程が、前記第１の制御および前記第２の制御に従って前記第１および第２のデータアイテムの前記複合体に対する動作を管理する工程を包含する、請求項352に記載の方法。

357．前記提供する工程が、前記第１の制御間の前記関連づけの完全性を確保する工程を包含し、前記第１のデータアイテムが、該第１のデータアイテムの送信、格納および処理の少なくとも１つにおいて維持される、請求項352に記載の方法。

358．前記提供する工程が、前記第１の制御とは個別に前記第１のデータアイテムを配送する工程を包含する、請求項352に記載の方法。

359．前記提供する工程が、前記第１のデータアイテムおよび前記第１の制御を共配送する工程を包含する、請求項352に記載の方法。

360．保護された動作を制御する安全な方法であって、

（ａ）少なくとも第１の制御および第２の制御を配送する工程と、

（ｂ）該第１および第２の制御の組み合わせに少なくとも部分的に基づいて少なくとも１つの保護された動作を制御する工程とを包含し、

以下の工程：

予め定義された順序に基づいて該第１および第２の制御間の少なくとも１つの衝突を解決する工程、

ユーザとのインタラクションを提供して該組み合わせを形成する工程、および

該第１および第２の制御間で動的にネゴシエートする工程、

の少なくとも１つを包含する方法。

361．前記制御する工程（ｂ）が、電子コンテンツの復号化を制御する工程を包含する、請求項358に記載の方法。

362．保護された電子コンテンツをパーティから受け取る工程と、

該受け取った保護された電子コンテンツを用いる前に該パーティのIDを認証する工程と、

をさらに包含する、請求項358に記載の方法。

363．保護されたデータを選択する工程と、

該保護されたデータをオブジェクトから抽出する工程と、

少なくとも１つの制御を同定し、該抽出したデータの使用の少なくとも１つの局面を管理する工程と、

該抽出したデータを他のオブジェクトに配置する工程と、

該少なくとも１つの制御と該他のオブジェクトとを関連づける工程と、

を包含する安全な方法。

364．前記少なくとも１つの制御に基づいて前記他のオブジェクトの使用の少なくとも１つの局面を制限する工程をさらに包含する、請求項361に記載の方法。

365．保護されたオブジェクトを改変する安全な方法であって、

（ａ）保護されたオブジェクトを提供する工程と、

（ｂ）少なくとも１つの他のエレメントを該保護されたオブジェクトに該オブジェクトを脱保護しないで埋め込む工程と、

を包含する安全な方法。

366．少なくとも１つの制御と前記オブジェクトとを関連づける工程と、

該制御に従って該エレメントの使用を制限する工程と、

をさらに包含する、請求項60に記載の方法。

367. 前記オブジェクト内のパーミッション記録をさらに有する、請求項363に記載の方法。

368. 前記オブジェクトを少なくとも部分的に暗号化する工程をさらに包含する、請求項364に記載の方法。

369. 安全な動作環境を用いて少なくとも１つのリソースを管理する方法であって、

該動作環境の外部にある第１のエンティティから第１のロードモジュールを安全に受け取る工程と、

該動作環境の外部にある第２のエンティティから第２のロードモジュールを安全に受け取る工程であって、該第２のエンティティが該第１のエンティティとは異なる工程と、

少なくとも１つのリソースを用いて、該第１および第２のロードモジュールに関連づけられたデータアイテムを安全に処理する工程と、

該第１および第２のロードモジュールを安全に適用し、該データアイテムと共に使用される該リソースを管理する工程と、

を包含する方法。

370. 電子契約をネゴシエートする方法であって、

遠隔サイトから第１の制御セットを受け取る工程と、

第２の制御セットを提供する工程と、

該第１の制御セットと該第２の制御セットとの間の電子ネゴシエーションを保護された処理環境内で実施する工程であって、該第１および第２の制御セット間にインタラクションを提供する工程を包含する工程と、

該第１および第２の制御セット間の該インタラクションから生じるネゴシエートされた制御セットを製造する工程と、

を包含する方法。

371. 電子商取引を支持するシステムであって、

第１のロケーションにおいて第１の安全な制御を作成する手段と、

第２のロケーションにおいて第２の安全な制御を作成する手段と、

該第１のロケーションから該第２のロケーションに該第１の安全な制御セットを安全に通信させる手段と、

該第１および第２の制御セットを安全に統合し、電子値チェーン延長契約を共に含む複数のエレメントを有する少なくとも第３の制御セットを製造する、該第２のロケーションにおける手段と、

を有するシステム。

372. 電子商取引を支持するシステムであって、

第１のロケーションにおいて第１の安全な制御を作成する手段と、

第２のロケーションにおいて第２の安全な制御を作成する手段と、

該第１のロケーションからの該第２のロケーションに該第１の安全な制御セットを安全に通信させる手段と、

該第１および第２の安全な制御セットの少なくとも一部を安全に実行させて電子契約をネゴシエートする該第２のロケーションにおけるネゴシエーション手段と、

を有するシステム。

373. 前記第１および／または第２の制御セットの少なくとも一部に基づいて、保護された情報コンテンツのユーザによる使用を制御する手段をさらに有する、請求項370に記載のシステム。

374. 前記コンテンツの使用の少なくとも一部に対して請求する手段をさらに有する、請求項370に記載のシステム。

375. 安全な構成要素をベースとした動作システムであって、

少なくとも１つの構成要素を検索する構成要素検索手段と、

構成要素アセンブリを指定する記録を検索する記録検索手段と、

該構成要素検索手段および該記録検索手段に操作によって連結される、該構成要素および／または該記録の有効性をチェックするチェック手段と、

該チェック手段に連結される、該記録に従って該構成要素を用いて該構成要素

アセンブリを形成する使用手段と、

該使用手段に連結される、該構成要素アセンブリに少なくとも部分的に基づいてプロセスを実施する実施手段と、

を有するシステム。

376. 安全な構成要素をベースとした動作システムであって、

少なくとも１つの構成要素および構成要素アセンブリを指定する少なくとも１つの記録を安全なデータベースから検索するデータベースマネージャーと、

該構成要素および／または該記録の有効性をチェックする認証マネージャーと、

該記録に従って該構成要素を使用して該構成要素アセンブリを形成するチャネルマネージャーと、

該構成要素アセンブリに少なくとも部分的に基づいてプロセスを実施する実行マネージャーと、

を有するシステム。

377. 安全な構成要素動作システムであって、

構成要素を検索する手段と、

該構成要素の使用を指定する指令を受け取って構成要素アセンブリを形成する手段と、

該受け取り手段に連結される、該受け取った構成要素および／または該指令を認証する手段と、

該認証手段に連結される、該受け取った指令に少なくとも部分的に基づいて該構成要素を用いて該構成要素アセンブリを形成する手段と、

該形成手段に連結される、該構成要素アセンブリを用いて少なくとも１つの動作を実施する手段と、

を有するシステム。

378. 安全な構成要素動作環境であって、

構成要素および該構成要素の使用を指定する指令を格納し、構成要素アセンブリを形成する格納デバイスと、

該構成要素および／または該指令を認証する認証マネージャーと、

該構成要素を用いて、該指令に少なくとも部分的に基づいて該構成要素アセンブリを形成するチャネルマネージャーと、

該構成要素アセンブリを実行し、少なくとも１つの動作を実施するチャネルと、

を有する環境。

379．安全な動作システムであって、

コードおよび該コードのアセンブリを指定する指令を実行可能なプログラムに格納する格納デバイスと、

該受け取ったコードおよび／または該アセンブリディレクタの有効性をチェックする有効性装置と、

イベントの発生に応答して、該アセンブリ指令に従って該コードを組み立て、実行用のアセンブリを形成するイベントで駆動されるチャネルと、

を有するシステム。

380．少なくとも１つのリソースを管理する安全な動作環境システムであって、

該動作環境の外部にある第１のエンティティから第１の制御を安全に受け取り、該動作環境の外部にある第２のエンティティから第２の制御を安全に受け取る通信配置であって、該第２のエンティティが該第１のエンティティとは異なる通信配置と、

該通信配置に連結される保護された処理環境であって、

（ａ）少なくとも１つのリソースを用いて該第１および第２の制御に関連づけられたデータアイテムを安全に処理し、

（ｂ）該第１および第２の制御を安全に適用し、該データアイテムを用いるための該リソースを管理する保護された処理環境と、

を有するシステム。

381．電子契約をネゴシエートするシステムであって、

遠隔サイトから受け取った第１の制御セットを格納し、第２の制御セットを格納する格納配置と、

該格納配置に連結される保護された処理環境であって、

（ａ）該第１の制御セットと該第２の制御セットとの間で電子ネゴシエーションを実施し、

（ｂ）該第１および第２の制御セット間にインタラクションを提供し、

（ｃ）該第１および第２の制御セット間の該インタラクションから生じるネゴシエートされた制御セットを製造する保護された処理環境と、

を有するシステム。

382．前記ネゴシエートされた制御セットを電子的に実施する手段をさらに有する、請求項379に記載のシステム。

383．前記ネゴシエートされた制御セットに基づいて電子契約を発生する手段をさらに有する、請求項379に記載のシステム。

384．電子商取引を支持する方法であって、

第１のロケーションにおいて第１の安全な制御セットを作成する工程と、

第２の安全な制御セットを作成する工程と、

該第１のロケーションとは異なる該ロケーションにおいて電子契約を電子的にネゴシエートする工程であって、該第１および第２の制御セットの少なくとも一部を安全に実行する工程を包含する工程と、

を包含する方法。

385．電子機器であって、

プロセッサと、

該プロセッサに接続された少なくとも１つのメモリデバイスとを有し、

該プロセッサが、

少なくとも１つの構成要素および構成要素アセンブリを指定する少なくとも１つの記録を該メモリデバイスから検索する検索手段と、

該検索手段に連結される、該構成要素および／または該記録の有効性をチェックするチェック手段と、

該検索手段に連結される、該記録に従って該構成要素を用いて該構成要素アセンブリを形成する使用手段と、

を有する電子機器。

386. 電子機器であって、

少なくとも１つのプロセッサと、

該プロセッサに接続された少なくとも１つのメモリデバイスと、

該プロセッサに操作によって連結される少なくとも１つの入力／出力接続とを有し、

該プロセッサが、権利オペレーティングシステムを少なくとも部分的に実行して該電子機器内に安全な動作環境を提供する電子機器。

387. 前記プロセッサがチャネルを提供する手段を有し、該チャネルが配送可能な構成要素を独立して構成要素アセンブリに組み立て、該構成要素アセンブリを実行する、請求項384に記載の電子機器。

388. 前記プロセッサに連結された二次的な格納デバイスをさらに有し、該二次的な格納デバイスが安全なデータベースを格納し、該プロセッサが該安全なデータベースから得られる情報を復号化し、該安全なデータベースに書き込まれる情報を暗号化する手段を有する、請求項384に記載の電子機器。

389. 前記プロセッサおよび前記メモリデバイスが、安全な不正改変不可能なカプセル化に配置される、請求項384に記載の電子機器。

390. 前記プロセッサがハードウェア暗号化器／復号化器を有する、請求項384に記載の電子機器。

391. 前記プロセッサがリアルタイムクロックを有する、請求項384に記載の電子機器。

392. 前記プロセッサが乱数発生器を有する、請求項384に記載の電子機器。

393. 前記メモリデバイスが監査情報を格納する、請求項384に記載の電子機器。

394. 安全な動作環境を用いて少なくとも１つのリソースの使用を監査する方法であって、

該動作環境の外部にある第１のエンティティから第１の制御を安全に受け取る工程と、

該動作環境の外部にある第２のエンティティから第２の制御を安全に受け取る

工程であって、該第２のエンティティが該第１のエンティティとは異なる工程と、

少なくとも１つのリソースを用いる工程と、

該リソースの使用に関する第１の監査情報を該第１の制御に従って該第１のエンティティに安全に送る工程と、

該リソースの使用に関する第２の監査情報を該第２の制御に従って該第２のエンティティに安全に送る工程であって、該第２の監査情報が該第１の監査情報とは少なくとも部分的に異なる工程と、

を包含する方法。

395．安全な動作環境を用いて少なくとも１つのリソースの使用を監査する方法であって、

該動作環境の外部にあるエンティティから第１および第２の制御代替を安全に受け取る工程と、

該第１および第２の制御代替の１つを選択する工程と、

少なくとも１つのリソースを用いる工程と、

該第１の制御代替が該選択工程によって選択される場合に、該リソースの使用に関する第１の監査情報を該第１の制御代替に従って該エンティティに安全に送る工程と、

該第２の制御代替が該選択工程によって選択される場合に、該リソースの使用に関する第２の監査情報を該第２の制御代替に従って該第２のエンティティに安全に送る工程であって、該第２の監査情報が該第１の監査情報とは少なくとも部分的に異なる工程と、

を包含する方法。

396．ユーザに予め配布された保護されたデジタル情報の販売を有効にする方法および／またはシステムであって、該情報に関連づけられた電子制御に基づいて該保護されたデジタル情報へのアクセスを選択的に制御する安全なエレメントによって特徴づけられる方法および／またはシステム。

397．補償と交換に商品および／またはサービスを選択的に放出する安全な処理

エレメントによって特徴づけられる、配布された安全な電子販売ポイントシステムまたは方法。

398. 分散されたデジタルネットワークにおいて、デジタル情報と該情報へのアクセスおよび／または該情報の使用に関する１つまたはそれ以上の制御とを関連づけている該デジタル情報の使用を追跡する工程と、該追跡に少なくとも部分的に基づいて広告メッセージを標的づける工程とによって特徴づけられる広告方法。

399. 前記システムが、相互作用可能な保護された処理環境の配送されたネットワークを用いて、広告を少なくとも部分的にユーザに配送することによって特徴づけられる分散された電子広告システム。

400. 配布された安全な仮想ブラックボックスであって、VDEコンテンツコンテナ作成者に配置されるノードと、他のコンテンツプロバイダと、クライアントユーザと、安全なVDEコンテンツ使用情報サイトの受け手とを有し、該仮想ブラックボックスのノードが、VDE制御プロセスを安全に実行する半導体素子または他のハードウェアモジュールなどの少なくとも１つの安全なハードウェア素子を有する安全なサブシステムを有し、該安全なサブシステムが、情報格納、配布、支払い、使用および／または監査の通路に沿ってノードに配布される仮想ブラックボックス。

401. 多数の通貨および／または安全な処理のための支払い配置を提供する工程と、保護されたデジタル情報を放出する工程とを包含する保護された処理システムまたは方法。

402. ユーザの年齢が、該ユーザに情報および／またはリソースを電子的に安全に放出するための基準として使用されることによって特徴づけられる配布された安全な方法またはシステム。

403. 安全な処理環境を定義する電子機器を貸す方法。

404. 以下の特徴および／またはエレメントおよび／またはその組み合わせの１つまたはそれ以上を提供する仮想配布環境であって、

構成可能な保護された分散されたイベント管理システム、および／または

信頼される配布された処理および格納管理配置、および／または

情報を提供し、情報を制御し、および／または報告するための複数の通路、および／または

多数の支払いメソッド、および／または

多数の通貨、および／または

EDI、および／または

電子銀行業務、および／または

電子文書管理、および／または

電子安全通信、および／または

電子メール、および／または

配布された非同期報告、および／または

組み合わせ非同期およびオンライン管理、および／または

ユーザによるプライバシ制御、および／または

テスト、および／または

クラスとしての年齢の使用、および／または

器具制御（貸し等）、および／または

テレコミュニケーションインフラストラクチャ、および／または

ゲーム管理、および／または

電子コンテナからのコンテンツの抽出、および／または

コンテンツの電子コンテナへの埋め込み、および／または

鍵の不履行を可能にする多数の証明書、および／または

仮想ブラックボックス、および／または

制御情報のコンテンツからの独立、および／または

１つのデジタル情報プロパティに対する多数の分離された同時制御セット、および／または

すでに配布されたデジタル情報に対する制御情報の更新、および／または

組織情報管理、および／または

処理と制御の連結された外部および組織内部チェーン、および／または

コンテンツ使用結果管理システム（報告、支払い等、多数の指令）、および／または

コンテンツ内に権利を保持する多数のパーティに向かう異なる監査情報および／または削減を提供するコンテンツ使用報告システム、および／または

自動化された遠隔安全オブジェクト作成システム、および／または

不適切な使用を同定するインフラストラクチャバックグラウンド分析、および／または

制御情報システムの順序判定、および／または

規則および制御が適用されるコンテンツとは個別の規則および制御の安全な配布および実施、および／または

再配布され得る権利、および／またはコピーおよび／またはピース等の数を制御することによる再配布管理、および／または

電子商取引課税システム、および／または

電子ショッピングシステム、および／または

電子カタログシステム、および／または

電子銀行業務、電子ショッピング、および電子コンテンツ使用管理を処理するシステム、および／または

電子商取引マルチメディアシステム、および／または

分散された安全な電子販売ポイントシステム、および／または

広告、および／または

電子権利管理、および／または

分散された電子商取引システム、および／または

配布された取引システムまたは環境、および／または

分散されたイベント管理システム、および／または

分散された権利システム

を提供する仮想配布環境。

405. 実質的に図１に示される仮想配布環境。

406. 実質的に図１Aに示される「情報ユティリティ」。

４０７．実質的に図１に示される処理と制御のチェーン。

４０８．実質的に図２Ａに示される持続的な規則および制御情報。

４０９．実質的に図１に示される異なる制御情報を提供する方法。

４１０．実質的に図４に示される規則および／または制御情報。

４１１．実質的に図５Ａおよび図５Ｂに示されるオブジェクト。

４１２．実質的に図６に示される安全な処理ユニット。

４１３．実質的に図７に示される電子機器。

４１４．実質的に図８に示される電子機器。

４１５．実質的に図９に示される安全な処理ユニット。

４１６．実質的に図１０に示される「権利オペレーティングシステム（"ＲＯＳ"）」アーキテクチャ。

４１７．実質的に図１１Ａから図１１Ｃに示されるアプリケーションと権利オペレーティングシステムとの間の機能関係。

４１８．実質的に図１１Ｄから図１１Ｊに示される構成要素および構成要素アセンブリ。

４１９．実質的に図１２に示される権利オペレーティングシステム。

４２０．実質的に図１２Ａに示されるオブジェクト作成方法。

４２１．実質的に図１３に示される「保護された処理環境」ソフトウェアアーキテクチャ。

４２２．実質的に図１５に示されるチャネルを支持する方法。

４２３．実質的に図１５Ａに示されるチャネルヘッダおよびチャネル詳細記録。

４２４．実質的に図１５Ｂに示されるチャネルを作成する方法。

４２５．実質的に図１６に示される安全なデータベース。

４２６．実質的に図１７に示される論理オブジェクト。

４２７．実質的に図１８に示される静止オブジェクト。

４２８．実質的に図１９に示される移動オブジェクト。

４２９．実質的に図２０に示されるコンテンツオブジェクト。

４３０．実質的に図２１に示される管理オブジェクト。

431. 実質的に図22に示されるメソッドコア。

432. 実質的に図23に示されるロードモジュール。

433. 実質的に図24に示されるユーザデータエレメント(UDE)および／またはメソッドデータエレメント(MDE)。

434. 実質的に図25Aから図25Cに示されるマップ計量器。

435. 実質的に図26に示されるパーミッション記録(PERC)。

436. 実質的に図26Aおよび図26Bに示されるパーミッション記録(PERC)。

437. 実質的に図27に示されるシッピングテーブル。

438. 実質的に図28に示される受け取りテーブル。

439. 実質的に図29に示される管理イベントログ。

440. 実質的に図30に示されるオブジェクト登録テーブル、主題テーブル、およびユーザ権利テーブルを相関させて用いる方法。

441. 実質的に図34に示されるサイト記録テーブルおよびグループ記録テーブルを用いて、安全なデータベースの部分を追跡する方法。

442. 実質的に図35に示される安全なデータベースを更新するプロセス。

443. 実質的に図36に示される新しいエレメントを安全なデータベースに挿入するプロセス。

444. 実質的に図37に示される安全なデータベース内のエレメントにアクセスするプロセス。

445. 実質的に図38に示される安全なデータベースエレメントを保護するプロセス。

446. 実質的に図39に示される安全なデータベースをバックアップするプロセス。

447. 実質的に図40に示される安全なデータベースを回収するプロセス。

448. 実質的に図41Aから図41Dに示される相互メソッドを実施することが、処理と制御のチェーンを提供することを可能にするプロセス。

449. 実質的に図42Aから図42Dに示される「相互」予算方法。

４５０．実質的に図４４Ａから図４４Ｃに示される相互監査方法。

４５１．実質的に図４５から図４８に示されるコンテンツの放出を制御する方法または他の方法。

４５２．実質的に図５３Ａから図５３Ｂに示されるイベントメソッド。

４５３．実質的に図５３Ｃに示される課金メソッド。

４５４．実質的に図５７Ａに示される抽出メソッド。

４５５．実質的に図５７Ａに示される埋め込みメソッド。

４５６．実質的に図５８Ａに示される不明瞭なメソッド。

４５７．実質的に図５８Ｂに示される指紋刻印メソッド。

４５８．実質的に図５８Ｃに示される指紋刻印メソッド。

４５９．実質的に図６に示される計量メソッド。

４６０．実質的に図６２に示される鍵旋回プロセス。

４６１．実質的に図６３に示される鍵旋回プロセスを用いて異なる鍵を生成して「真」の鍵を決定するプロセス。

４６２．実質的に図６４および／または図６５に示される保護された処理環境鍵を初期化するプロセス。

４６３．実質的に図６６に示される静止オブジェクト内に含まれる情報を復号化するプロセス。

４６４．実質的に図６７に示される移動オブジェクト内に含まれる情報を復号化するプロセス。

４６５．実質的に図６８に示される保護された処理環境を初期化するプロセス。

４６６．実質的に図６９に示される保護された処理環境にファームウェアをダウンロードするプロセス。

４６７．実質的に図７０に示されるネットワークまたは他の通信手段と共に接続された多数のＶＤＥ電子機器。

４６８．実質的に図７１によって示されるポータブルＶＤＥ電子機器。

４６９．実質的に図７２Ａから図７２Ｄに示されるユーザ通知および例外インターフェースによって生成され得る「ポップアップ」表示。

４７０．実質的に図７３によって示されるスマートオブジェクト。

４７１．実質的に図７４によって示されるスマートオブジェクトを処理する方法。

４７２．実質的に図７５Ａから図７５Ｄに示される電子ネゴシエーション。

４７３．実質的に図７５Ｅから図７５Ｆに示される電子契約。

４７４．図７６Ａから図７６Ｂのいずれかに実質的に示される電子ネゴシエーションプロセス。

４７５．実質的に図７７に示される処理と制御のチェーン。

４７６．実質的に図７８に示されるＶＤＥ「格納場所」。

４７７．実質的に図７９から図８３のいずれかまたはすべてに示される処理と制御のチェーンを用いてＶＤＥで管理されたコンテンツおよび制御情報を発展および変換するプロセス。

４７８．実質的に図８４に示されるＶＤＥ参加者のいくつかのカテゴリを含む処理と制御のチェーン。

４７９．実質的に図８５に示される組織内の配布と処理のチェーン。

４８０．実質的に図８６および／または図８６Ａに示される処理と制御のチェーン。

４８１．実質的に図８７に示される仮想シリコンコンテナモデル。

４８２．ビジネス自動化方法であって、（ａ）暗号化された決算および／または他の管理情報コンテンツを含む１つまたはそれ以上の安全なコンテナを作成する工程と、（ｂ）制御情報と、該１つまたまそれ以上の安全なコンテナの１つまたはそれ以上とを関連づける工程であって、該制御情報が、（ｉ）該１つまたはそれ以上のコンテナの１つまたはそれ以上を使用し得る１つまたはそれ以上のパーティおよび（ｉｉ）該決算および／または他の管理情報に対する１つまたはそれ以上のパーティに対して実施される動作の記述を含む、工程と、（ｃ）該１つまたはそれ以上のコンテナの１つまたはそれ以上を該１つまたはそれ以上のパーティに電子的に配送する工程と、（ｄ）保護された処理環境を用いて、該制御情報の少なくとも一部の実施を有効にする工程とによって特徴づけられる方法。

４８３．ビジネス自動化システムであって、

関連づけられた制御情報を有する管理情報コンテンツを有する少なくとも１の安全なコンテナを提供する手段と、

少なくとも部分的に該制御情報を実施する保護された処理環境と、

によって特徴づけられるシステム。

484．ビジネス自動化システムであって、（ａ）配布された相互作用可能な保護された処理環境インストレーションと、（ｂ）デジタル情報を配布するための安全なコンテナと、（ｃ）処理と制御機能のチェーンの自動化を支持する制御情報とを有するシステム。

485．ビジネス自動化方法であって、相互作用可能な保護された処理環境ノードを複数のパーティに提供する工程と、第１のパーティから第２のパーティに第１の暗号化されたデジタル情報を通信させる工程と、該第１の通信されたデジタル情報の少なくとも一部および／または該第１のデジタル情報の使用に関連する情報を含む第２の暗号化されたデジタル情報を該第１または第２のパーティとは異なる第３のパーティに通信させる工程とによって特徴づけられ、該第２の暗号化されたデジタル情報の使用が、該第３のパーティに得られる相互作用可能な保護された処理環境によって少なくとも部分的に制御される方法。

486．ビジネス自動化システムであって、

複数の保護された処理環境ノードと、

該ノード間でデジタル情報を通信させる手段とによって特徴づけられ、

該ノードの少なくとも１つが、該通信されたデジタル情報の使用を制御する手段を有するシステム。

487．処理と制御のチェーン方法であって、（ａ）第１のパーティが、保護されたデジタル情報を第１のソフトウェアコンテナに配置し、該デジタル情報の少なくとも一部の使用を管理する規則および制御を規定する工程と、（ｂ）該ソフトウェアコンテナを第２のパーティに提供する工程とを包含し、該第２のパーティが、該ソフトウェアコンテナを他のソフトウェアコンテナに配置し、第３のパーティによる該デジタル情報の少なくとも一部および／または該第１のソフトウェアコンテナの使用を少なくとも部分的に管理するための規則および制御を規定す

る方法。

488. 処理と制御のチェーンシステムであって、

デジタル情報を第１のソフトウェアコンテナに配置し、該デジタル情報の少なくとも一部の使用を管理する規則および／または制御を規定する手段と、

該ソフトウェアコンテナを他のソフトウェアコンテナに配置し、該デジタル情報の少なくとも一部および／または該第１のソフトウェアコンテナの使用を少なくとも部分的に管理するための他の規則および／または制御を規定する手段と、

によって特徴づけられるシステム。

489. 処理と制御のチェーンシステムであって、（ａ）少なくとも部分的に保護されたデジタル情報を含む第１のコンテナと、（ｂ）該デジタルコンテンツの少なくとも一部を使用するための条件を確立する第１のパーティによって規定される少なくとも部分的に保護された制御情報と、（ｃ）該第１のコンテナとは異なり、該第１のコンテナを含む第２のコンテナと、（ｄ）該第２のコンテナのコンテンツの使用を管理するための条件を少なくとも部分的に設定する第２のパーティによって独立して規定される制御情報とを有するシステム。

490. 電子広告システムであって、（ａ）デジタル情報をユーザに該ユーザが使用するために提供する手段と、（ｂ）広告コンテンツを該デジタル情報と組み合わせて該ユーザに提供する手段と、（ｃ）該デジタル情報の使用を監査する手段と、（ｄ）広告コンテンツの使用に関する使用情報を安全に得る手段と、（ｅ）該広告コンテンツ使用情報に基づいて情報を安全に報告する手段と、（ｆ）該広告コンテンツの使用に少なくとも部分的に基づいて少なくとも１つのコンテンツプロバイダを補償することを有するシステム。

491. 電子広告方法であって、（ａ）デジタル情報をコンテナに配置する工程と、（ｂ）広告情報と、該デジタル情報の少なくとも一部とを関連づける工程と、（ｃ）該コンテナをコンテナユーザに安全に提供する工程と、（ｄ）広告情報をユーザが見ることをモニタする工程と、（ｄ）広告者から支払いを受け取る工程とを包含し、該支払いが該広告情報をユーザが見ることと関連する方法。

492. 電子広告システムであって、（ａ）コンテンツおよび広告情報の両方を有

するデジタル情報をコンテナ化する手段と、（ｂ）該広告情報の少なくとも一部を見ることをモニタする手段と、（ｃ）該広告情報の少なくとも一部をユーザが見ることに対して請求する手段と、（ｄ）安全なコンテナにおける該見ることに基づいた情報を安全に通信させる手段と、（ｅ）該見ることに基づいた該情報の通信を管理するための該コンテナ化されたデジタル情報に関連する制御情報とを有するシステム。

493．電子広告方法であって、（ａ）コンテンツおよび広告情報の両方を有するデジタル情報をコンテナ化する工程と、（ｂ）該広告情報の少なくとも一部をユーザが見ることをモニタする工程と、（ｃ）該広告情報の少なくとも一部をユーザが見ることに対して請求する工程と、（ｄ）安全コンテナにおける該見ることに基づいた情報を安全に通信させる手段と、（ｅ）該広告情報に関連する制御情報を用いて、該見ることに基づいて情報の通信少なくとも部分的に管理する工程とによって特徴づけられる方法。

494．取扱情報をクリアする方法であって、（ａ）相互作用可能な保護された処理環境の第１のユーザにデジタル情報を安全に配布する工程と、（ｂ）該第１のユーザとは異なる相互作用可能な保護された処理環境のユーザに他のデジタル情報を安全に配布する工程と、（ｃ）該デジタル情報の使用に関連する情報を受け取る工程と、（ｄ）該他のデジタル情報の使用に関連する情報を受け取る工程と、（ｅ）工程（ｃ）および（ｄ）に従って受け取られた情報を処理して、（Ｉ）管理または(II)分析機能の少なくとも１つを実施する工程とによって特徴づけられる

方法。

495．取扱情報をクリアするシステムであって、（ａ）少なくとも部分的に保護されたデジタル情報および関連づけられた制御情報を含む第１のコンテナと、（ｂ）少なくとも部分的に保護された他のデジタル情報および関連づけられた制御情報を含む第２の安全なコンテナと、（ｃ）該第１および第２のコンテナをユーザに配布する手段と、（ｄ）該第１のコンテナデジタル情報のユーザ使用から少なくとも部分的に引き出される情報を通信させる通信手段と、（ｅ）該第２のコ

ンテナデジタル情報のユーザ使用から少なくとも部分的に引き出される情報を通信させる通信手段と、（ｆ）工程（ｄ）および（ｅ）を通して通信される該情報を受け取る情報交換所サイトにおける処理手段とを有し、該処理手段が、該通信された情報の少なくとも一部の管理および／または分析処理を実施するシステム。

496．情報交換所分析方法であって、（ａ）配布され、少なくとも部分的に保護されたデジタル情報の使用を管理および／または分析する複数の独立した情報交換所を有効にする工程と、（ｂ）相互作用可能な保護された処理環境を複数の独立したユーザに提供する工程と、（ｃ）ユーザが、相互作用可能な保護された処理環境と共に用いるための情報交換所を選択することを可能にする工程とによって特徴づけられる方法。

497．情報交換所分析システムであって、（ａ）配布され、少なくとも部分的に保護されたデジタル情報の使用を管理および／または分析する複数の独立した情報交換所と、（ｂ）複数のユーザロケーションのそれぞれにおける少なくとも１つの相互作用可能な保護された処理環境と、（ｃ）ユーザが、該複数の独立した情報交換所の１つを選択し、該少なくとも部分的に保護されたデジタル情報の該使用に関連する支払いおよび／または分析機能を実施することを可能にする選択手段とを有する情報交換所分析システム。

498．電子広告方法であって、

１つまたはそれ以上の電子広告を作成し、該広告の少なくとも一部を含む１つまたはそれ以上の安全なコンテナを作成する工程と、

制御情報と該広告とを関連づける工程であって、該制御情報が、（ａ）少なくともいくらかの広告使用情報を１つまたはそれ以上のコンテンツプロバイダ、広告者および／またはエージェントに報告すること、（ｂ）該広告の該ユーザによる見ることおよび／または他の使用に基づいて、１つまたはそれ以上の貸し方をユーザに提供すること、（ｃ）広告使用情報を１つまたはそれ以上の市場分析者に報告すること、（ｄ）１つまたはそれ以上の製品および／またはサービスを注文する注文情報および／または手段をユーザに提供する工程と、および／または

（ｅ）該広告の１つまたはそれ以上のユーザによる見ることおよび／または他の使用に基づいて、１つまたはそれ以上の貸し方をコンテンツプロバイダに提供することの少なくとも１つを記述する制御情報を含む工程と、

該コンテナおよび該制御情報を１つまたはそれ以上のユーザに提供する工程と、

該ユーザが、少なくとも部分的に該制御情報に従って該コンテナを使用することを可能にする工程と、

によって特徴づけられる方法。

499．電子広告システムであって、（ａ）デジタル情報をユーザに該ユーザが使用するために提供する手段と、（ｂ）広告コンテンツを該デジタル情報と組み合わせて該ユーザに提供する手段と、（ｃ）該デジタル情報の使用を監査する手段と、（ｄ）広告コンテンツの使用に関する使用情報を安全に得る手段と、（ｅ）該広告コンテンツ使用情報に基づいて情報を安全に報告する手段と、（ｆ）該広告コンテンツの使用に少なくとも部分的に基づいて少なくとも１つのコンテンツプロバイダを補償することを有するシステム。

500．処理と制御のチェーンシステムであって、（ａ）少なくとも部分的に保護されたデジタル情報を含む第１のコンテナと、（ｂ）該デジタルコンテンツの少なくとも一部を使用するための条件を確立する第１のパーティによって規定される少なくとも部分的に保護された制御情報と、（ｃ）該第１のコンテナと異なり、該第１のコンテナを含む第２のコンテナと、（ｄ）該第２のコンテナのコンテンツの使用を管理するための条件を少なくとも部分的に設定する第２のパーティによって独立して規定される制御情報とを有するシステム。

501．情報交換所を動作させる方法であって、複数のパーティからの安全なコンテナの使用に少なくとも部分的に関連する使用情報を受け取る工程と、該使用情報に少なくとも部分的に基づいて１つまたはそれ以上のパーティに支払われるべき支払いを決定する工程と、該決定に少なくとも部分的に基づいて該パーティへの支払いに導かれる取扱を実施するおよび／または実施させる工程とによって特徴づけられる方法。

５０２．電子情報交換所であって、

複数のパーティからの安全なコンテナの使用に少なくとも部分的に関連する使用情報を受け取る手段と、

該使用情報に少なくとも部分的に基づいて１つまたはそれ以上のパーティに支払われるべき支払いを決定する手段と、

該決定に少なくとも部分的に基づいて該パーティへの支払いに導かれる取扱を実施するおよび／または実施させる手段と、

を有する電子情報交換所。

５０３．情報交換所を動作させる方法であって、複数のパーティからの安全なコンテナの使用に少なくとも部分的に関連する使用情報を受け取る工程と、該使用情報に少なくとも部分的に基づいて１つまたはそれ以上のパーティが使用するレポートを決定する工程と、該決定に少なくとも部分的に基づいて使用のレポートを作成および／または作成させる工程と、該レポートの少なくとも１つを該パーティの少なくとも１つに配送する工程とによって特徴づけられる方法。

５０４．情報交換所を動作させる方法であって、パーミッションおよび／または少なくとも１つの安全なコンテナ内の少なくとも１つの権利の他のパーティへの配送を可能にする情報を有する１つまたはそれ以上のコンテンツプロバイダからの他の制御情報を受け取る工程と、１つまたはそれ以上の安全なコンテナにおける１つまたはそれ以上の権利に対するリクエストを複数のパーティから受け取る工程と、該リクエストに少なくとも部分的に基づいて、パーミッションおよび／または他の制御情報を該パーティに配送する工程とによって特徴づけられる方法。

５０５．情報交換所を動作させる方法であって、パーティのＩＤ情報を確立する１つまたはそれ以上のパーティから情報を受け取る工程と、少なくとも１つの安全なコンテナ内で少なくとも１つの権利を有効にするおよび／または抑制するのに用いられる該ＩＤ情報の少なくとも一部の１つまたはそれ以上の電子表現を作成する工程と、該電子表現を証明する動作を実施する工程と、該電子表現を該パーティに配送する工程とによって特徴づけられる方法。

５０６．情報交換所を動作させる方法であって、安全なコンテナと共に用いるため

のパーティからの貸し方に対するリクエストを受け取る工程と、該リクエストに少なくとも部分的に基づいて貸し方の量を決定する工程と、該量に関連する制御情報を作成する工程と、該制御情報を該ユーザに配送する工程と、該貸し方の使用に関連する使用情報を受け取る工程と、該ユーザからの支払いの回収に関連づけられた少なくとも１つの取扱を実施および／または実施させる工程とによって特徴づけられる方法。

507．電子値チェーンに対して安全な制御情報を与える方法であって、制御情報が該値チェーンに直接関与しないパーティによって与えられ、該与えられた制御情報と、電子値チェーンにおいて１つまたはそれ以上のパーティによって規定されるデジタル情報に関連づけられた制御情報とを合計する工程であって、該合計制御情報が、該デジタル情報の少なくとも一部の使用に関連する条件を少なくとも部分的に管理する工程を包含する方法。

508．商取引イベントに関連づけられた税金の支払いをエンターする方法であって、該商取引イベントの税金支払いを自動的に管理するための安全な制御情報がパーティによって与えられ、該安全な制御情報と、個別のパーティによって与えられた制御情報とを合計する工程と、デジタル情報を使用するための少なくとも１つの条件を制御する工程とを包含する方法。

509．汎用の再利用可能な電子商取引配置方法であって、

（ａ）制御されたイベントを含むように共に構成され得る構成要素構造、モジュラメソッドを提供する工程と、

（ｂ）統合可能な保護された処理環境を複数の独立したユーザに提供する工程と、

（ｃ）統合可能な保護された処理環境間でデジタル制御情報を通信させる安全な通信手段を用いる工程と、

（ｄ）該提供された構成要素モジュラメソッドの少なくとも一部を格納する該処理環境に操作によって接続されるデータベースマネージャーを有効にする工程と、

によって特徴づけられる方法。

５１０．汎用の再利用可能な電子商取引システムであって、

（ａ）イベント制御構造を含むように共に構成される構成要素モジュラメソッドと、

（ｂ）複数の独立したユーザロケーションのそれぞれにおける少なくとも１つの相互作用可能な処理環境と、

（ｃ）相互作用可能な保護された処理環境間でデジタル制御情報を通信させる安全な通信手段と、

（ｄ）該構成要素モジュラメソッドの少なくとも一部を格納する該保護された処理環境に操作によって接続される安全なデータベースマネージャーと、

を有するシステム。

５１１．汎用の電子商取引貸し方システムであって、

（ａ）安全な相互作用可能な保護された処理環境と、

（ｂ）少なくとも部分的に保護されたデジタル情報をユーザが使用するための貸し方を提供するための汎用の貸し方制御情報と、

（ｃ）該汎用の貸し方制御情報を少なくとも部分的に使用して貸し方を用いるために必要な情報を提供するための少なくとも部分的に保護されたデジタル情報に関連する制御情報と、

を有するシステム。

５１２．汎用の電子商取引貸し方システムを有効にする方法であって、

（ａ）安全な相互作用可能な保護された処理環境を提供する工程と、

（ｂ）少なくとも部分的に保護されたデジタル情報をユーザが使用するための貸し方を提供するための汎用の貸し方制御情報を供給する工程と、

（ｃ）該汎用の貸し方制御情報を少なくとも部分的に使用して貸し方を用いるために必要な情報を提供するための少なくとも部分的に保護されたデジタル情報に関連する制御情報と、

を包含する方法。

５１３．１つまたはそれ以上のSPUを含む１つまたはそれ以上の電子機器および該SPUの少なくとも１つに操作によって接続される１つまたはそれ以上の安全なデー

タベースを有する文書管理システム。

514．１つまたはそれ以上のSPUを含む１つまたはそれ以上の電子機器および該SPUの少なくとも１つに操作によって接続される１つまたはそれ以上の安全なデータベースを有する電子契約システム。

515．少なくとも１つのSPUおよび該SPUに操作によって接続される少なくとも１つの安全なデータベースを有する電子機器。

516．１つまたはそれ以上のCPUを有し、該CPUの少なくとも１つが少なくとも１つのSPUと統合される電子機器。

517．１つまたはそれ以上のビデオコントローラを有し、該ビデオコントローラの少なくとも１つが少なくとも１つのSPUと統合される電子機器。

518．１つまたはそれ以上のネットワーク通信手段を有し、該ネットワーク通信手段の少なくとも１つが少なくとも１つのSPUと統合される電子機器。

519．１つまたはそれ以上のモデムを有し、該モデムの少なくとも１つが少なくとも１つのSPUと統合される電子機器。

520．１つまたはそれ以上のCD-ROMデバイスを有し、該CD-ROMデバイスの少なくとも１つが少なくとも１つのSPUと統合される電子機器。

521．１つまたはそれ以上のセットトップコントローラを有し、該セットトップコントローラの少なくとも１つが少なくとも１つのSPUと統合される電子機器。

522．１つまたはそれ以上のゲームシステムを有し、該ゲームシステムの少なくとも１つが少なくとも１つのSPUと統合される電子機器。

523．少なくとも１つのマイクロプロセッサと、メモリと、入力／出力手段と、情報を暗号化および／または復号化する少なくとも１つの回路と、暗号化および／または復号化関数を実施する該マイクロプロセッサの少なくとも１つと共に用いられる１つまたはそれ以上のソフトウェアとを有する多重暗号化アルゴリズムを支持する集積回路。

524．少なくとも１つのマイクロプロセッサと、メモリと、少なくとも１つのリアルタイムクロックと、少なくとも１つの乱数発生器と、情報を暗号化および／

または復号化する少なくとも１つの回路と、独立して配送されおよび／または独立して配送可能な証明されたソフトウェアを有する集積回路。

525. 少なくとも１つのマイクロプロセッサと、メモリと、入力／出力手段と、不正改変不可能なバリアと、権利オペレーティングシステムの少なくとも一部とを有する集積回路。

526. 少なくとも１つのマイクロプロセッサと、メモリと、入力／出力手段と、少なくとも１つのリアルタイムクロックと、不正改変不可能なバリアと、該リアルタイムクロックの少なくとも１つにパワーの中断を記録する手段とを有する集積回路。

【発明の詳細な説明】

安全な取引管理および電子権利保護のためのシステムおよび方法

発明の分野

本発明は、概して、コンピュータおよび／または電子セキュリティに関する。

より詳細には、本発明は、安全な取引管理のためのシステムおよび技術に関する。本発明はまた、情報へのアクセス、および／または情報の使用が承認された方法のみでおこなわれることを保証するコンピュータベースおよび他の電子機器ベースの技術にも関し、本発明によってそのような使用に関連するそのような情報およびプロセスの完全性、利用可能性、および／または機密性が維持される。

本発明はまた、電子商取引および他の電子取引または電子的に促進される取引における様々な参加者の権利を保護するためのシステムおよび方法に関する。

本発明はまた、情報コンテンツ、およびそのようなコンテンツの使用およびそのような使用結果を規制するために用いられる情報のための取扱いおよび制御の安全なチェーンに関する。また、本発明は、電子的に格納されたおよび／または配信された情報の使用の計量および／または制限および／またはモニタを含む管理を行う、システムおよび技術に関する。本発明は、特に、そのようなシステムおよび／または技術の使用の結果を含む、そのようなシステムおよび／または技術を利用する取引、運営および取り決めに関する。

本発明はまた、分散型および他のオペレーティングシステム、環境およびアーキテクチャに関する。また、本発明は、概して、例えば、分散型システムの各ノードでセキュリティを確立するために用いられ得る、例えば、不正改変不可能なハードウェアベースのプロセッサを含む安全なアーキテクチャに関する。

発明の背景および要旨

現在、遠隔通信、金融取引、行政手続、業務作業、娯楽、および個人事業生産のすべてが、電子機器に依存している。これらの何百万もの電子機器が電子的に互いに接続されている。これらの相互接続された電子機器は、次第に「情報ハイウエイ」と称されるようになっているものを備えている。多くの企業、学者および政治指導者が、この情報（「電子的」あるいは「ディジタル」である）ハイウ

エイを用いる市民および組織の権利をどのように保護するかを案じている。

電子コンテンツ

今日では、単語、数字、図形、またはコマンドおよび命令体系によって表され得るものは事実上すべて、電子ディジタル情報にフォーマット化され得る。テレビ、ケーブル、衛星伝送、および電話線を通って伝送されるオンラインサービスは、家庭および企業へのディジタル情報および娯楽の配布をするために競合している。このコンテンツの所有者および販売者には、ソフトウェア開発者、動画およびレコード会社、本、雑誌および新聞の出版社、情報データベースプロバイダが含まれる。オンラインサービスの大衆化によって、個人のパーソナルコンピュータユーザがコンテンツのプロバイダとして参加することも可能になった。Microsoft Corporationによると、1992年の電子情報の世界規模の市場は約400億ドルであり、1997年までに2000億ドルまでに増加することが見込まれていると見積もられている。本発明は、コンテンツプロバイダの総収入を大幅に増加させ、配布コストおよびコンテンツのコストを大幅に下げ、広告および使用情報収集をよりよくサポートし、電子情報ユーザの要求をより満足させることを可能にする。これらの改善によって、電子情報の量および種類ならびにそのような情報が配布される方法が大幅に増加する。

従来の製品が電子情報プロバイダおよびユーザの要求に合い得ないことは、本発明と明確な差をなす。アメリカの最も大きい代表的な遠隔通信、コンピュータ、娯楽および情報プロバイダ会社は、本発明によって述べられる問題のうちの幾つかに目を向けたが、本発明のみが、構成可能な汎用電子商取引／配布制御システムのための商業的に安全で且つ効果的な解決方法を提供する。

電子コンテンツの制御

本発明は、電子情報使用を安全化し、管理し、監査する新しい種類の「仮想配布環境（virtual distribution environment）」（本明細書において、「VDE」と称する）を提供する。VDEはまた、「情報ハイウエイ」を「通る」コンテンツ

を管理する、基本的に重要なケーパビリティを特徴とする。これらのケーパビリティは、すべての電子共同体メンバーに役立つ権利保護解決法を含む。これらの

メンバーは、コンテンツのクリエータおよび配布者、金融サービスプロバイダ、エンドユーザ、その他を含む。VDEは、コンピュータ、他の電子機器、ネットワークおよび情報ハイウエイのユーザのための最初の構成可能な汎用取引制御／権利保護解決法である。

電子コンテンツプロバイダが有する根本的な問題は、所有権のある情報の使用を制御する能力を拡張することである。コンテンツプロバイダは、承認された活動および量に使用を制限する必要がしばしばある。例えば、映画の配給および光ディスクの広告に関する企業モデルの参加者には、役者、監督、脚本家およびその他のライター、音楽家、撮影所、出版社、配布者、小売り人、広告者、クレジットカードサービス、およびコンテンツエンドユーザが含まれ得る。これらの参加者は、使用制限を含む契約および要件の範囲を、電子企業モデル全体を含む「拡張された」契約に具現化する能力が必要となる。この拡張された契約は、権利および義務によって自動的に契約を強制し得る電子コンテンツ制御情報によって表される。VDE下では、そのような拡張された契約は、すべての企業モデル参加者を含む電子契約を含み得る。またはあるいはさらに、そのような契約は、企業モデル参加者のサブセット間の電子契約から構成され得る。VDEを用いることによって、電子取引は従来の取引と同様に機能し得る。すなわち、商品およびサービスに関する商業関係は、様々なパーティ間の１つ以上の契約のネゴシ.エーションによって実現され得る。

商業的なコンテンツプロバイダは、それらの電子情報の使用の適切な補償を保証することに執心している。例えば、CD録音である電子ディジタル情報は、今日、比較的容易かつ安価にコピーされ得る。同様に、権利を有する所有者は、International Intellectual Property Allianceによると、ソフトウェアプログラムの非許可コピーおよび使用によって、歳入で何十億ドルの損害を被る。コンテンツプロバイダおよび配布者は、自分自身の権利を保護するために数多くの制限された機能権利保護メカニズムを考案した。より流布したコンテンツ保護スキームのうちのいくつかには、承認パスワードおよびプロトコル、ライセンスサーバ、

「ロック／ロック解除」配布方法、および収縮包装された（shrink-wrapped）ソ

フトウェアのユーザに課せられる非電子契約制限がある。商業的コンテクストでは、これらの労力は効果的ではなく、制限された解決法となっている。

「電子通貨」のプロバイダも、このタイプのコンテンツに対する保護を作り出した。これらのシステムは、一般的な電子通貨の使用をサポートするほどに、十分に適合可能でも、効率的でも、フレキシブルでもない。さらに、これらのシステムは、精巧な監査および制御構成ケーパビリティを提供しない。これは、現在の電子通貨ツールが、現実世界の多くの金融企業モデルに必要である精巧さを欠いていることを意味している。VDEは匿名の通貨および「条件つき」匿名である通貨のための手段を提供し、この場合、通貨に関連する活動は、特別な状況下にある以外は匿名のままである。

VDE制御ケーパビリティ

VDEによって、電子ディジタル情報の所有者および配布者が電子情報の使用に対する課金を信頼性をもって行うこと、および電子情報の使用を安全に制御し、監査し、かつ予算を作成することが可能になる。これによって、市販の情報製品の使用を信頼性をもって検出およびモニタし得る。VDEは、例えば、ディジタルネットワーク、ディジタル放送、および光ディスクおよび磁気ディスクのような物理的な記憶媒体を含む、幅広い異なる電子情報配送手段を使用する。VDEは、主要なネットワークプロバイダ、ハードウェア製造者、電子情報の所有者、そのような情報のプロバイダ、および電子情報に関する使用情報を収集し、電子情報の使用に対して課金を行う情報交換所（clearinghouse）によって用いられ得る。

VDEは、包括的かつ構成可能な取引管理、計量、およびモニタ技術を提供する。VDEは、電子情報製品の保護方法、販売方法、包装方法、および配布方法を変え得る。使用時には、VDEは、情報プロバイダに、より大きな歳入をもたらし、ユーザに、より大きな満足および価値を与えるべきてある。VDEの使用によって、通常、使用コストおよび取引コストが低くなり、電子情報へのアクセスがより効率的になり、権利保護およびその他の取引管理実施が再利用可能になり、安全化された情報の使用におけるフレキシビリティが大幅に改善され、電子取引管理に

ついてのツールおよびプロセスがより標準化される。VDEは、電子情報所有者、配布者、およびユーザ；金融情報交換所；ならびに使用情報分析者および転売者の要求を満たす適合可能な環境を作るために用いられ得る。

権利および制御情報

本発明は、概して以下を有するパーティの権利を保護するために用いられ得る：

（ａ）電子情報における所有権または機密的利益。これによって、例えば、情報が承認された方法のみで用いられることが保証され得る；

（ｂ）電子的に配布された情報の使用によって生じる金融利益。これによって、コンテンツプロバイダは配布された情報の使用に対して支払いを受けることが保証され得る；

（ｃ）電子クレジットおよび電子通貨保管、通信、および／または電子キャッシュ、バンキングおよび購入を含む使用における利益。

電子共同体メンバーの権利の保護には、広範な技術が関連している。VDEは、「分散型の」電子権利保護「環境」を作り出すように、これらの技術を組み合わせる。この環境は、権利保護に重要な取引および他のプロセスを安全化し、および保護する。例えば、VDEは、重要な権利に関連する取引およびプロセスの防止、あるいは妨害、干渉および／または観察を提供する。好ましい実施の形態において、VDEは、VDEプロセスならびに情報格納および通信について高レベルのセキュリティを提供し得るようにするために、特殊目的不正改変不可能な安全処理ユニット（SPU）を用いる。

本発明によって解決される権利保護問題は、基本的な社会問題を電子的な面で考えたものである。これらの問題は、財産権の保護、プライバシー権の保護、人々および組織の仕事およびリスクについての適切な補償、金銭およびクレジットの保護、および情報のセキュリティの包括的な保護を含む。VDEは、効率的で信用のあるコスト的に有効な方法で権利問題を管理するために、共通した組のプロセスを用いるシステムを使用している。

VDEは、例えば、レコード、ゲーム、映画、新聞、電子ブックおよび参考資料

、個人電子メール、ならびに機密記録および通信などの電子コンテンツを作成するパーティの権利を保護するために用いられ得る。本発明はまた、出版社および配布者などの電子製品を供給するパーティの権利；例えば、クレジット情報交換所および銀行などの、製品の使用について支払いを行うための電子クレジットおよび通貨を供給するパーティの権利；電子コンテンツを用いるパーティ（消費者、実業家、政府など）のプライバシーに対する権利、および医学的記録、税金記録あるいは個人記録に含まれている情報に関するプライバシー権などの電子情報によって示されるパーティのプライバシー権を保護するために用いられ得る。

本発明は、概して以下を有するパーティの権利を保護し得る：

（ａ）電子的に配布された情報の商業的利益。本発明は、例えば、パーティが、彼らの契約と一致する方法で、配布された情報の使用に対して支払いを受けることを保証し得る；

（ｂ）電子情報における所有権および／または機密的利益。本発明は、例えば、データが承認された方法のみで安全に用いられるようにし得る；

（ｃ）電子クレジットおよび電子通貨保管、通信、および／または使用における利益。これは、電子キャッシュ、バンキングおよび購入を含み得る；および

（ｄ）少なくとも一部が他の電子情報の使用から得られる電子情報における利益。

VDE機能特性

VDEは、取引処理を安全化し管理するための、統一された一貫的なシステムを提供する、コスト的に有効で効率的な権利保護解決法である。VDEは以下のことを行い得る。

（ａ）コンテンツの使用を監査および分析する、

（ｂ）コンテンツが承認された方法のみで用いられることを保証する、

（ｃ）コンテンツユーザによって許可された方法のみで、コンテンツ使用に関する情報を使用し得るようにする。

さらに、VDEは、

（ａ）構成可能性、改変性および再利用性が高い；

（ｂ）ほとんどの潜在的なアプリケーションを提供するために種々の方法で組み合わされ得る、広範囲の有用なケーパビリティをサポートする；

（ｃ）手持ち可能な安価な装置から大型のメインフレームコンピュータにわたる広い範囲の電子機器上で動作する；

（ｄ）多数の異なるパーティの様々な権利および多数の異なる権利保護スキームを同時に保証し得る；

（ｅ）異なる時間および異なる場所で生じ得る一連の取引を介してパーティの権利を保護し得る；

（ｆ）情報を安全に配送し、使用を報告する種々の方法をフレキシブルに受け入れ得る；および、

（ｇ）商品およびサービスに対する支払いを行うため、かつ、個人（家庭を含む）のバンキングおよび他の金融活動をサポートするために、匿名の電子キャッシュを含む、「本物の」金銭およびクレジットの電子類似物を提供する。

VDEは、電子共同体メンバーの権利保護要求を経済的かつ効率的に満たす。VDEのユーザは、異なる情報ハイウエイ製品および権利問題のための付加的な権利保護システムを必要とせず、また、新しい情報ハイウエイアプリケーションについての新しいシステムをインストールおよび学習する必要もない。

VDEは、すべてのコンテンツクリエータ、プロバイダおよびユーザが同一の電子権利保護解決法を用いることを可能にする統一された解決法を提供する。承認された状況下では、参加者は、コンテンツおよび関連付けられたコンテンツ制御セットを自由に交換し得る。これは、VDEのユーザが、許可された場合、異なるセットのコンテンツ制御情報を有する異なる種類のコンテンツと共に作動するために同一の電子システムを用い得ることを意味している。ある一つのグループによって供給されるコンテンツおよび制御情報は、通常は異なるグループによって供給されるコンテンツおよび制御情報を用いる人々によって用いられ得る。VDEによってコンテンツが「普遍的に」交換され得、本発明を実施するユーザは、コンテンツ制御における非互換性に対する懸念、権利の侵害、または新しいコンテンツ制御システムを入手、インストールまたは学習することを必要とせずに電子

的に相互作用し得る。

VDEは、権利の保護を指定する取引を安全に管理する。これは、例えば、以下を含む電子権利を保護し得る：

（ａ）電子コンテンツの作者の所有権、

（ｂ）コンテンツの配布者の商業的権利、

（ｃ）コンテンツの配布を促進させた任意のパーティの権利、

（ｄ）コンテンツのユーザのプライバシー権、

（ｅ）保管されたおよび／または配布されたコンテンツによって表されるパーティのプライバシー権、

（ｆ）電子契約の施行に関するその他の任意の権利。

VDEは、非常に幅広い電子的に施行された商業的および社会的契約を可能にし得る。これらの契約は、電子的に実施される契約、ライセンス、法律、規則および税金徴収を含み得る。

従来の解決法との対比

従来のコンテンツ制御メカニズムは、ユーザが必要とするあるいは望むよりも多くの電子情報をユーザが購入することをしばしば要求する。例えば、収縮包装されたソフトウェアをたまにしか用いないユーザは、あまり頻繁に用いないことではるかに少ない見返りしか受け取り得ないにもかかわらず、頻繁に使用するユーザと同一の価格でプログラムを購入する必要がある。従来のシステムは、使用程度または使用の性質に従ってコストを決定せず、購入可能性がある消費者は固定価格が高すぎると感じ、それらの消費者を引きつけ得ない。また、従来のメカニズムを用いるシステムは、通常、特別に安全なものではない。例えば、収縮包装は、いったん物理的パッケージまたは電子パッケージから取り出されると、不断のソフトウェアの違法著作権侵害を防止しない。

従来の電子情報権利保護システムはしばしばフレキシブルではなく、非効率的であり、これによってコンテンツプロバイダは費用のかかる配布チャネルを選択し、製品の価格が上昇する。一般的に、これらのメカニズムは、商品の価格決定、構成、および市場売買のフレキシビリティを制限する。これらの侵犯は、異なる

コンテンツモデル、およびコンテンツ配送戦略などのモデル参加者の多くの様々な要求を反映するコンテンツモデルの両方を受け入れ得ない情報を制御する技術があることによって生じる。これによって、多くの潜在的なユーザの面前で与えられた製品のコストを正当化するために十分な全体価値を配送する、プロバイダの能力が制限され得る。VDEによって、コンテンツプロバイダおよび配布者が、コンテンツプロバイダおよびユーザの好ましい企業モデルを反映するアプリケーションおよび配布ネットワークを製作することが可能になる。これによって、プロバイダの所望の情報配布方法およびユーザのそのような情報の所望の使用法をサポートする、一義的にコスト有効で、特徴に富んだシステムがユーザに提供される。VDEは、権利を保障し、かつ、最大の商業的成果のためにコンテンツ配送戦略を適合させ得るコンテンツ制御モデルをサポートする。

取扱いおよび制御のチェーン

VDEは、電子情報におけるあるいは電子情報に対する権利を有する様々なパーティに属する権利の収集を保護し得る。この情報は、一つの場所にあっても、複数の位置にわたって分散されていても（および／または複数の位置の間を移動しても）よい。情報は、配布者の「チェーン」およびユーザの「チェーン」を通って通過し得る。使用情報は、パーティの１つ以上の「チェーン」を通っても報告され得る。一般的には、VDEによって、（ａ）電子情報において権利を有し、および／または（ｂ）電子情報において権利を有するパーティのための直接的または間接的な代理人として働くパーティが、情報の移動、アクセス、改変または使用が、そのような活動がどのように、いつ、どこで、およびだれによって行われ得るかに関する規則によって、安全に制御され得ることを保証することができる。

VDEアプリケーションおよびソフトウェア

VDEは、電子処理および商取引を規制するための安全なシステムである。規制は、１つ以上のパーティによって適所に配置された制御情報によって保証される。これらのパーティは、コンテンツプロバイダ、電子ハードウェア製造者、金融サービスプロバイダ、またはケーブルあるいは遠隔通信会社などの電子「インフラ

ストラクチャ」企業を含み得る。制御情報は、「権利アプリケーション」を実施する。権利アプリケーションは、好ましい実施の形態の「基本ソフトウェア」上で「走る」。この基本ソフトウェアは、多くの異なる権利アプリケーション、すなわち、異なる企業モデルおよびそれらのそれぞれの参加者要求を受け入れ得る、安全でフレキシブルな汎用基礎（foundation）として働く。

VDE下での権利アプリケーションは、特別の目的を持つ部分から構成され、各部分は、権利保護環境のために必要とされる１つ以上の基礎的な電子プロセスに対応し得る。これらのプロセスは建築用ブロックのように組み合わせされ、それによって電子情報のユーザおよびプロバイダの権利を保護することができ、かつ、義務の遂行を実施させ得る電子契約が作られ得る。電子情報の１つ以上のプロバイダは選択された建築用ブロックを容易に組み合わせ、それによって特殊なコンテンツ配布モデルに特有の権利アプリケーションを作りだし得る。これらの部分のグループは、ユーザとプロバイダとの間の契約を遂行するために必要なケーパビリティを提示し得る。これらの部分は、以下を含む電子契約の多くの要件を受け入れ得る：

！　電子情報を使用するためのパーミッションの配布；

！　制御情報およびこれらのパーミッションを管理する制御情報のセットの持続性；

！　そのような情報と共に用いるためにユーザによって選択され得る構成可能な制御セット情報；

！　電子情報のデータセキュリティおよび使用監査；および、

！　通貨、補償、および借方（debit）管理のための安全なシステム。

電子商取引のためには、本発明の好ましい実施の形態においては、権利アプリケーションはすべての参加者の間での企業契約の電子的施行を提供し得る。異なるアプリケーションについて異なるグループのコンポーネントが組み立てられ得るので、本発明は、幅広い範囲の異なる製品および市場のために電子制御情報を供給し得る。これは、本発明が、電子商取引およびデータセキュリティのために「統合された」効率的な安全かつコスト有効なシステムを提供し得ることを意味している。これによって、VDEが電子権利保護、データセキュリティ、および電

子通貨および銀行業務のための単一の基準となることが可能になる。

VDEにおいて、権利アプリケーションとその基礎との間の分離によって、多くの異なるタイプのアプリケーションおよび使用のそれぞれについて適切な制御情報のセットを効率的に選択することが可能になる。これらの制御セットは、電子共同体メンバーの権利および義務（ある人物の製品の使用履歴の提供、またはある人物の電子購入に課せられる税金の支払いなど）の両方を反映し得る。VDEのフレキシビリティによって、VDEのユーザが共通の社会的および商業的倫理および慣習を電子的に実行および施行することができる。統一された制御システムを提供することによって、本発明は、個人、共同体、企業および政府の幅広い範囲の生じる可能性のある取引関連利益および関心事をサポートする。オープン設計であるので、VDEによって、ユーザによって独立して作り出された技術を用いたアプリケーションが（通常は、安全に制御された状況下で）システムに「付加され」、本発明の基礎と共に用いられることが可能になる。要するに、VDEは、パーティ間での契約を高く反映し施行し得るシステムを提供する。このシステムは、安全でコスト有効かつ公正な電子環境に対する差し迫った必要性に応える、幅広い体系的な解決法である。

VDE実施

本発明の好ましい実施の形態は、システム設計者にVDEケーパビリティの製品への直接の挿入を可能にする様々なツールを含む。これらのツールは、アプリケーションプログラマーズインタフェース（「API」）および権利パーミッションおよび管理言語（「RPML」）を含む。RPMLは、本発明の特徴の使用に対する包括的で詳細な制御を提供する。VDEはまた、コンテンツプロバイダ、配布者およびユーザの要求を満たすための、あるユーザインタフェースサブシステムも含む。

VDEを用いて配布される情報は、多くの形態をとり得る。例えば、情報は、個人自身のコンピュータ上で用いるために「配布」され得る。すなわち、本発明は、局所的に格納されたデータにセキュリティを与えるために用いられ得る。あるいは、1以上の受け手に対する著作者および／または出版社によってばらまかれる情報と共にVDEを用いてもよい。この情報は、以下を含む多くの形態をとり得る。

それらは、映画、音声録音、ゲーム、電子カタログショッピング、マルチメディア、トレーニング材料、Eメール、および個人文書、オブジェクト指向ライブラリ、ソフトウェアプログラミングリソース、および参照／記録維持情報リソース（企業データベース、医学データベース、法データベース、科学データベース、行政データベース、および消費者データベースなど）である。

本発明によって提供される電子権利保護はまた、信用があり効率的なホームバンキングおよび商業的バンキング、電子クレジットプロセス、電子購入、真の（true）または暫定的に匿名の電子キャッシュ、およびEDI（電子データ交換）に重要な基礎も提供する。VDEは、鍵およびパスワードベースの「go／no go」技術よりもはるかに有効であり得る「スマート」取引管理特徴を提供することによって、組織におけるデータセキュリティを改善するための重要な強化を行う。

VDEは通常、暗号手法技術およびその他のセキュリティ技術（例えば、暗号化、ディジタル署名など）と、コンポーネント型、分散型およびイベント起動されるオペレーティングシステム技術、ならびに関連する通信、オブジェクトコンテナ、データベース、スマートエージェント、スマートカード、および半導体設計技術を含む他の技術との統合を用いている。

I．概観

A．VDEは重要課題を解決し、重大な必要性を満たす。

世界は、電子情報機器の統合に向かって動いている。機器のこの相互接続によって、さらに大きな電子相互作用および電子取引の発展のための基礎を与える。様々なケーパビリティが、電子商取引環境を実施するために要求される。VDEは、これらのケーパビリティの多くを提供するので、従って、情報の電子配信に関連する基本的な問題を解決する最初のシステムである。

電子コンテンツ

VDEは、2つ以上のパーティを伴う電子的な取り決めを行うことを可能にする。これらの契約は、それ自体が、商業的な価値チェーンおよび／または取扱い、監査、報告および支払いのためのデータセキュリティチェーンモデルにおける参加

者間の契約の収集を含み得る。これによって、配布、使用制御、使用支払い、使用監査、および使用報告などの、安全な電子コンテンツのための有効で再利用可能かつ改変可能な一貫した手段が提供され得る。コンテンツは、例えば、以下を含む。

！　電子通貨およびクレジットなどの金融情報、

！　参照データベース、映画、ゲームおよび広告などの商業的に配布された電子情報、および

！　文書、Ｅメールおよび所有権データベース情報などの、個人および組織によって生じる電子プロパティ。

ＶＤＥによって、異なる競合する企業の提携、契約、および発展する企業モデル全体をサポートする電子商取引市場が可能になる。

ＶＤＥの特徴によって、ＶＤＥは、大量の従来の電子商取引およびデータセキュリティ要件に合い、それらをサポートし得る最初の信用のある電子情報制御環境として機能し得る。特に、ＶＤＥによって、企業価値チェーンモデルにおける参加者が従来の企業契約約定および条件の電子バージョンを作り出し、さらに、これらの参加者が企業要件に対して適切であると考えるように電子商取引モデルを適合させ発展させることが可能になる。

ＶＤＥは、特定の配布の偏り、管理および制御見通し、およびコンテンツタイプを反映することを避けるアーキテクチャを提供する。その代わりに、ＶＤＥは、広いスペクトルの、基本的に構成可能で移植可能な（ｐｏｒｔａｂｌｅ）電子取引制御、配布、使用、監査、報告および支払い動作環境を提供する。ＶＤＥは、電子相互作用活動および参加者の制限されたサブセットのみをカバーするアプリケーションまたはアプリケーションに特定的なツールセットに限られない。むしろ、ＶＤＥは、そのようなアプリケーションが作成、改変および／再利用され得るシステムをサポートする。その結果、本発明は、プログラム可能で安全な電子取引管理基礎および再利用可能で拡張可能な実行可能コンポーネントの使用によって、電子機器の相互動作性、コンテンツコンテナの相互動作性、および電子商取引アプリケーションおよびモデルの効率的な作成を促進する標準化された制御環境をサポートするシステムを提供し、それによって、差し迫った未解決の要求に応える。ＶＤＥ

は、電子取引活動の大半の形態が管理され得る単一の電子「世界」をサポートし得る。

権利所有者およびコンテンツプロバイダの高まる要求に応え、かつ、電子企業モデルに関わり得るすべてのパーティ（クリエータ、配布者、管理者、ユーザ、クレジットプロバイダなど）の要件および契約を受け入れ得るシステムを提供するために、VDEは効率的かつ大部分においてトランスペアレントで、低コストかつ十分に安全なシステム（ハードウェア／ソフトウェアモデルおよびソフトウェア限定モデルの両方をサポートする）を供給する。VDEは、以下に要求される広範な安全制御および管理ケーパビリティを提供する。

１．種々のタイプの電子コンテンツ、

２．異なる電子コンテンツ配送スキーム、

３．異なる電子コンテンツ使用スキーム、

４．種々のコンテンツ使用プラットホーム、および

５．異なるコンテンツ市場売買およびモデル戦略。

VDEは、多くの別々のコンピュータおよび／または他の電子機器と組み合わせ、または一体化され得る。これらの機器は、代表的には、表示、暗号化、復号化、印刷、コピー、保存、抽出、埋込み、配布、監査のためなどの使用のコンテンツ使用の制御を可能にし得る安全なサブシステムを含む。好ましい実施の形態における安全なサブシステムは、１つ以上の「保護下の処理環境」と、１つ以上の安全なデータベースと、安全な状態で維持されることが必要である安全な「コンポーネントアセンブリ」ならびに他のアイテムおよびプロセスとを備えている。例えば、VDEは、そのような「安全なサブシステム」を用いて、電子通貨、支払い、および／またはクレジット管理（電子クレジットおよび／または通貨受け取り、支払い、債務を課すこと、および／または配分を含む）を安全に制御し得る。

VDEは、電子的に供給および／または格納された情報の配布および／または他の使用を制御するための安全な分散電子取引管理システムを提供する。VDEは、電子コンテンツおよび／または機器使用の監査および報告を制御する。VDEのユ

ーザには、コンテンツ使用、使用報告、および／または使用支払いに関する制御情報を、エンドユーザ組織、個人、およびコンテンツおよび／または機器配布者などのユーザのための電子コンテンツおよび／または機器へ適用するコンテンツクリエータを含み得る。VDEはまた、電子クレジットおよび／または通貨の形態での、１つ以上のパーティが１つ以上の他のパーティに対して負う金銭（コンテンツおよび／または機器の使用に対して支払われる金銭を含む）の支払いをサポートする。

VDEの制御下の電子機器は、配布された電子情報および／または機器使用、制御情報公式化（formulation）、および関連する取引を安全に処理および制御するVDE「ノード」を表す。VDEは、２つ以上のパーティによって提供される制御情報の統合を安全に管理し得る。その結果、VDEは、２つ以上のパーティの制御要件間の「ネゴシエーション」を表すVDE参加者間の電子契約を構成し得、その結果行われる契約の約定および条件を規定する。VDEによって、電子情報および／または機器使用に関連する広範な電子活動に関する電子契約に対する各パーティの権利が保証される。

VDEの制御システムの使用を介して、従来のコンテンツプロバイダおよびユーザは、伝統的かつ非電子的な関係を反映する電子関係を確立し得る。コンテンツプロバイダおよびユーザは、プロバイダおよびユーザ間で大きくなる要求および彼らの間の契約に適応するように商業的関係を適合させ改変し得る。制限され大半が固定された機能性をサポートする計量および制御アプリケーションプログラムにあわせるために電子コンテンツプロバイダおよびユーザの企業規定および個人の好みを変えることを、VDEは電子コンテンツプロバイダおよびユーザに要求しない。さらに、VDEによって、例えば、コンテンツ使用情報の詳細な報告、今まで実行不可能であった低価格での多くの個別取引、参加者が関わることまたは参加者が事前に知っていることを必要とせずに実施される「パスアロング（pass-along）」制御を含む非電子取引と共に実行不可能な企業モデルを、参加者は発展させることができる。

本発明によって、コンテンツプロバイダおよびユーザは、以下に適合するよう

に取引環境を公式化し得る。

（１）所望のコンテンツモデル、コンテンツ制御モデル、およびコンテンツ使用情報経路、

（２）全ての範囲の電子メディアおよび配布手段、

（３）広範な価格設定、支払いおよび監査戦略、

（４）非常にフレキシブルなプライバシーおよび／または報告モデル、

（５）実用的かつ有効なセキュリティアーキテクチャ、および

（６）ステップ（１）～（５）と共に、電子世界に独特のモデルを含む大半の「現実世界の」電子商取引およびデータセキュリティモデルを可能にし得る、他の管理手続き。

VDEの取引管理ケーパビリティは以下を施行し得る。

（１）電子情報および／または機器の使用に関する情報に関連するプライバシー権、

（２）コンテンツユーザの権利を保護する、または電子取引設入から生じる税金徴収を必要とする法律などの社会的政策、

（３）電子情報の所有、配布および／または電子情報に関連する他の商業権に関連する、パーティの所有権および／または他の権利。

VDEは、「現実の」商取引を電子形態でサポートし得る。それは、価値チェーン企業モデルを表す相互関連契約のネットワークを経時的に形成する、商関係の進歩的な世界である。これは、一部には、安全に作成され、かつ独立して提出されたコンテンツおよび／または機器制御情報のセットの相互作用（それらの間のネゴシエーション）によってコンテンツ制御情報を発展させ得ることによって達成される。コンテンツおよび／または機器制御情報の異なるセットは、本発明により可能にされた電子企業価値チェーンにおいて異なるパーティによって提出され得る。これらのパーティは、それぞれのVDEインストレーション（設備）の使用によって制御情報セットを作成する。独立して安全に配送可能なコンポーネントベースの制御情報によって、異なるパーティによって供給される制御情報セット間での有効な相互作用が可能になる。

VDEによって、VDEにサポートされた電子価値チェーンモデルにおけるパーティのサブセット間で、複数の別々の電子協定を行うことが可能になる。これらの複数の契約は統合されると、VDE価値チェーン「拡張された」契約を含む。付加的なVDE参加者がVDEコンテンツおよび／または機器制御情報取扱いに関わるようになると、VDEによって、そのような構成を成す電子契約、従って、VDE拡張契約全体が経時的に発展および再適合し得る。VDE電子契約は、新しい制御情報が既存の参加者によって提出されても拡張され得る。VDEを用いると、取引参加者は、自分自身の電子商取引企業活動および関係を自由に構成および再構成し得る。その結果、VDEを用いることによって同一のまたは共有されるコンテンツを用いて異なった非常に様々な企業モデルが可能になるので、本発明によって、競合する電子商取引市場が発展し得る。

電子商取引を概してサポートする本発明の能力の重要な側面は、（通常は、1つ以上の方法、データ、ロードモジュールVDEコンポーネントを含むVDEオブジェクトの形態である）制御情報を含む独立して配送されたVDEコンポーネントオブジェクトを安全に管理する能力である。この独立して配送された制御情報は上位の(senior)他の既存のコンテンツ制御情報と統合され、本発明のネゴシエーションメカニズムを用いて誘導された制御情報を安全に形成し得る。この得られた制御情報によって指定されるすべての要件は、VDE制御されたコンテンツがアクセスまたは使用され得ないうちに満たされなければならない。これは、例えば、必要とされる得られた制御情報によって列挙されるすべてのロードモジュールおよびいずれもの介在データは、利用可能であり、かつ、それらの要求される機能を安全に行わなければならないことを意味している。本発明の別の側面と組み合わされると、安全に、独立して配送される制御コンポーネントによって、電子商取引参加者が、自分自身の企業要件およびトレードオフを自由に規定することが可能になる。その結果、従来の非電子商取引と同様に、本発明によって、（VDE参加者による様々な制御要件の進歩的な規定を介する）電子商取引が最も効率的で競合する有用な企業形態に発展し得る。

VDEは、電子商取引および電子取引管理のサポートを合理化するケーパビリテ

ィを提供する。この合理化は、取引管理に関連する広範な活動のための制御構造およびユーザインタフェースが再利用可能であることから生じる。その結果、コンテンツ使用制御、データセキュリティ、情報監査および電子金融活動は、再利用可能で、便利で一貫し普及しているツールを用いてサポートされ得る。さらに、合理的なアプローチー－取引／配布制御規格－－によって、VDEのすべての参加

者に対して、非常に様々なタイプの情報、企業市場モデル、および／または秘密目的をサポートするための、ハードウェア制御およびセキュリティ、オーサリング、管理および管理ツールの同一の基本セットが可能になる。

汎用電子取引／分散制御システムとしてVDEを用いることによって、ユーザは、各コンピュータ、ネットワーク、通信ノード、および／または他の電子機器上で単一の取引管理制御アレンジメントを維持し得る。このような汎用システムは、異なる目的のために個別に異なるインストレーション（設備）を必要とせずに、多くの電子取引管理アプリケーションの必要性を満たす。その結果、VDEのユーザは、各異なるコンテンツおよび／または企業モデルについて異なる制限された目的の取引制御アプリケーションの混乱、費用および他の不都合を避けることができる。例えば、コンテンツオーサリングのため、および商品へ含めるためあるいは他の使用について他のコンテンツクリエータからコンテンツをライセンス取得するために同一のVDE基礎制御構成を用いることが、VDEによってコンテンツクリエータに可能になる。情報交換所、配布者、コンテンツクリエータ、および他のVDEユーザはすべて、VDE活動のタイプとは無関係に、同一の配布ツール、メカニズム、および一貫したユーザインタフェースを（概してトランスペアレントに）利用および再利用して完全に一貫して、VDEインストレーションで動作するアプリケーションと相互動作し、かつ、互いに相互作用し得る。

電子的に格納され、および／または配布された情報の制御および監査（および使用のその他の管理）によって、VDEは電子情報が多くの形態で不許可使用されることを防止する。これは、例えば、市販されたコンテンツ、電子通貨、電子クレジット、企業取引（EDIなど）、機密通信などを含む。VDEはさらに、課金のた

めにコンテンツクリエータおよび／または他のプロバイダによって「予め決定された」コンテンツの部分をユーザが使用するように制限するのではなく、ユーザが規定した部分において商業的に供給された電子コンテンツをユーザに利用可能にするために用いられ得る。

VDEは、例えば、以下を利用し得る：

（１）電子コンテンツおよび／または機器使用の予算作成および／または監査するための安全な計量手段、

（２）支払い手段のための電子クレジットおよび／または通貨メカニズムを含む、コンテンツおよび／または機器使用についての補償および／または課金率を可能にする、安全でフレキシブルな手段；

（３）制御および使用に関連する情報を格納する（および有効であると認められた区分化およびタグ付けスキームを用いる）ための安全な配分されたデータベース手段；

（４）安全な電子機器制御手段；

（５）（VDEコンテンツコンテナクリエータ、他のコンテンツプロバイダ、クライアントユーザ、および安全なVDEコンテンツ使用情報の受け手を含む）すべてのユーザの所在地に位置するノードを含む、分散型の安全な「仮想ブラックボックス」。この仮想ブラックボックスのノードは、通常は、少なくとも一つの安全なハードウェア素子（半導体素子あるいはVDE制御プロセスを安全に実行するための他のハードウェアモジュール）を有する安全なサブシステムを含んでいる。安全なサブシステムは、情報格納、配布、支払い、使用および／または監査の経路に沿ってノードに分散されている。いくつかの実施の形態において、ハードウェア素子の機能は、ノードの一部あるいはすべてについて、例えば、電子機器のホスト処理環境においてソフトウェアによって行われ得る；

（６）暗号化および復号化手段；

（７）認証、ディジタル署名、および暗号化された伝送を用いる安全な通信手段。ユーザノードでの安全なサブシステムは、各ノードのおよび／または参加者のアイデンティティを確立および認証し、安全なサブシステム間での通信のため

の１つ以上の安全なホスト－ホスト暗号化鍵を確立するプロトコルを用いる；および、

（８）各VDEインストレーション毎に、VDEコンテンツオーサリング（関連づけられた制御情報を有するVDEコンテナへのコンテンツの配置）、コンテンツ配布、およびコンテンツ使用、ならびにコンテンツ使用情報を用いて情報交換所およびその他の管理活動および分析活動を行うことを可能にし得る安全な制御手段。

VDEは、大半の非電子的な従来の情報配送モデル（娯楽、参考資料、カタログショッピングなどを含む）を、安全なディジタル配布および使用管理および支払いコンテクストに適切に移行させるために用いられ得る。VDE構成によって管理される分散および金融経路は、以下を含む：

！　コンテンツクリエータ、

！　配布者、

！　再配布者、

！　クライアント管理者、

！　クライアントユーザ、

！　金融情報交換所および／またはその他の情報交換所、

！　および／または行政機関。

これらの配布経路および金融経路はまた、以下を含み得る：

！　広告者、

！　市場調査組織、および／または

！　VDEを用いて安全に配送されたおよび／または格納された情報のユーザ使用に関心を持つその他のパーティ。

通常は、VDE構成における参加者は、同一の安全なVDE基礎を用いる。別の実施の形態は、異なるVDE基礎を用いるVDE構成をサポートする。このような別の実施の形態は、ある相互動作要件が満たされることを保証するためにプロシジャを用い得る。

安全なVDEハードウェア（安全処理ユニットを表すSPUとしても知られる）または、ソフトウェアを用いてハードウェア（ホスト処理環境（HPE）によって提供さ

れる）VDEに替わるまたは補足するVDEインストレーションは、本発明の電子契約／権利保護環境を達成するために、安全な通信、システム統合ソフトウェア、および配布ソフトウェア制御情報およびサポート構造と共同して動作する。これらのVDEコンポーネントは全体として、安全な、仮想、配布コンテンツおよび／または機器制御、監査（および他の管理）、報告および支払い環境を含む。商業的に許容可能ないくつかの実施の形態において、十分に物理的に安全な非VDE処理環境を通常維持する情報交換所などのある種のVDE参加者は、VDEハードウェアエレメントではなくHPEを用い、例えば、VDEエンドユーザおよびコンテンツプロバイダと相互動作することが可能であり得る。VDEコンポーネントは全体で、電子

コンテンツおよび／または機器使用の、分散型の非同期的な制御のための、構成可能で一貫した安全で「信頼される」アーキテクチャを含む。VDEは、電子コンテンツ配送、広範囲な配信、使用報告および使用に関連する支払い活動のための「全世界的な」環境をサポートする。

VDEは、一般化された構成可能性を提供する。これは、一部には、電子商取引およびデータセキュリティをサポートするための一般化された要件を、様々に集まって電子商取引アプリケーション、商業電子契約およびデータセキュリティ構成のためのコントロールメソッドを形成し得る広範な構成要素となり得る、「原子」レベルおよびそれよりも高レベルのコンポーネント（ロードモジュール、データエレメント、およびメソッドなど）に分解することによって生じる。VDEは、電子商取引モデルおよび関係を発展させ得る、安全な独立して配送可能なVDEコンポーネントと共にVDE基礎エレメントを用いる、安全な動作環境を提供する。VDEは、後続のコンテンツプロバイダおよび／またはユーザが電子コンテンツおよび／または電子機器の使用のためおよびその使用結果として、制御情報の適合化に参加することに対してコンテンツプロバイダが経時的に合意を明示し得る、あるいはそれを許可し得る配布モデルの開放を、特にサポートする。電子商取引およびデータセキュリティ活動を単純なものから非常に複雑なものまでサポートするために重要な非常に広範な機能属性は、本発明のケーパビリティによってサポートされる。その結果、VDEは、大半のタイプの電子情報および／または機

器、すなわち、使用制御（配分を含む）、セキュリティ、使用監査、報告、他の管理および支払い構成をサポートする。

好ましい実施の形態において、VDEは、（少なくとも一部が）暗号化または安全化されている情報の配送のための「コンテナ」を形成するためにオブジェクトソフトウェア技術を用い、オブジェクト技術を用いる。これらのコンテナは、電子コンテンツ製品あるいは他の電子情報およびそれらの関連するパーミッション（制御）情報の一部あるいはすべてを含み得る。これらのコンテナオブジェクトは、コンテンツプロバイダおよび／またはコンテンツユーザに関連する経路に沿って配分され得る。これらは、仮想配布環境（VDE）構成のノードの間を安全に移動し得る。これらのノードは、VDE基礎ソフトウェアを動作させ、コントロールメソッドを実行することによって電子情報使用制御および／または管理モデルを成立させる。本発明の好ましい実施の形態を使用することによって配送されるコンテナは、VDE制御命令（情報）を配布するため、および／または少なくとも一部が安全化されたコンテンツをカプセル化し電子的に配布するための両方に用いられ得る。

本発明を用いるコンテンツプロバイダには、例えば、ソフトウェアアプリケーションおよびゲーム発行者、データベース発行者、ケーブル、テレビおよびラジオ放送者、電子ショッピング販売者、および電子文書、本、定期刊行物、Eメールおよび／またはその他の形態での情報の配布者が含まれる。電子情報の格納者および／または配布者として働く法人(corporations)、行政機関および／または個人の「エンドユーザ」は、VDEコンテンツプロバイダであってもよい（制限されたモデルでは、ユーザはコンテンツを自分自身のみに供給し、別のパーティによる非許可使用から自分自身の機密情報を守るためにVDEを用いる）。電子情報は、個人的な使用または内部組織での使用のための所有権および／または機密情報、ならびに他のパーティに供給され得るソフトウェアアプリケーション、文書、娯楽材料、および／または参考情報を含み得る。配布は、例えば、「スタティック」ファイルおよび／またはデータストリームの形態での、物理的媒体配送、放送および／または遠隔通信手段によって行われ得る。VDEはまた、例えば、通

信された情報の一部またはすべての使用に対する制限および／または監査が実施される電子会議、インタラクティブゲーム、またはオンライン掲示板などのマルチサイト「リアルタイム」インタラクションのために用いられ得る。

VDEは、商業契約を実施し、かつ、プライバシー権の保護を可能にするための重要なメカニズムを提供する。VDEは、販売された電子コンテンツの使用に関してある一つのパーティから別のパーティに情報を安全に配送し得る。そのようなコンテンツ使用情報のための取扱いのチェーン（経路）におけるいくつかの「段階」によってパーティが分離される場合でも、そのような情報は暗号化および／または別の安全な処理を介してVDEによって保護される。その保護があるために、そのような情報が正確であることはVDEによって保証され、情報が配送されるすべてのパーティから情報が信用され得る。さらに、そのような情報は承認された

パーティまたはそのエージェントのみが復号化し得るように暗号化されているので、この情報は意図され承認されたパーティ以外によって受け取られ得ないことをすべてのパーティが信用し得ることがVDEによって保証される。このような情報は、前の取扱い経路位置において安全なVDE処理を介して得られ、それによって安全なVDE報告情報を生成し、次いでこの情報は、意図された受け手のVDE安全サブシステムに安全に通信され得る。VDEはそのような情報を安全に配送し得るので、電子契約を行うパーティは、VDEの制御下にある手段以外の手段を介して配送される商業的使用情報および／または他の情報の正確さを信用する必要はない。

商業的価値チェーン中のVDE参加者は、VDEを用いることによって結ばれた直接的な（構成する）および／または「拡張された」電子契約が信頼性をもって実施され得ることを「商業的に」信頼し得る（すなわち、商業目的には十分に信頼し得る）。これらの契約は、電子情報および／または機器使用の予算作成、計量および／または報告によって実施されるコンテンツ使用制御情報などの「動的な」取引管理に関連する側面を有しても、および／またはサービスに対する支払い、コンテンツまたはシステムの使用から得られる電子情報を非許可パーティに渡さ

ない、および／または著作権を守ることに同意するなどの「静的」電子主張を含んでもよい。電子的に報告された取引に関連する情報が本発明によって信用され得るだけではなく、支払い経路（報告のための経路と同じでも同じでなくともよい）を介した支払いトークンの通過によって支払いが自動化され得る。このような支払いは、VDE制御電子コンテンツおよび／または機器（行政機関、金融クレジットプロバイダ、およびユーザなど）に基づいて電子アカウント（例えば、ユーザのVDEインストレーション安全サブシステムによって安全に維持されるアカウント）からのクレジットまたは電子通貨（トークンなど）の「引き出し」を規定する制御情報（好ましい実施の形態においては、１つ以上のパーミッションレコード内に配置されている）に応答して、VDEインストレーションによって自動的に生成されたVDEコンテナ内に含まれ得る。

VDEによって電子商取引参加者の要求が満たされ、そのような参加者全体を、非常に大きな商取引をサポートするために十分に安全であり得る世界規模の信用

される商業ネットワーク中でまとめ得る。VDEのセキュリティおよび計量安全サブシステムコア(core)は、VDEに関連するコンテンツが（ａ）割当てられた使用に関連する制御情報（規則および調停データ）であり、および／または（ｂ）使用される、すべての物理的位置に存在する。このコアは、「仮想ブラックボックス」と称される、安全化された情報交換（例えば、遠隔通信）プロセスおよび分散されたデータベース手段によって相互接続された分散型の非常に安全なVDE関連ハードウェアの例の集まり内で動作するセキュリティおよび監査機能（計量を含む）を行い得る。VDEはさらに、高度に構成可能な取引オペレーティングシステム技術、提携されたデータを伴うロードモジュールの１つ以上の関連ライブラリ、VDE関連管理、データ準備および分析アプリケーション、ならびにホスト環境及びアプリケーションへのVDE統合を可能にするように設計されたシステムソフトウェアを含む。VDEの使用制御情報は、例えば、プロパティコンテンツおよび／または機器に関連する、使用承認、使用監査（監査割引も含み得る）、使用課金、使用支払い、プライバシーの漏洩、報告およびセキュリティに関連する通信および暗号化技術を提供する。

VDEは、VDE環境の構成性、移植可能性およびセキュリティを向上させるためにソフトウェアオブジェクト形態の方法を広範囲に用いる。VDEはまた、保護下のコンテンツを保持するVDEコンテンツコンテナのためのソフトウェアオブジェクトアーキテクチャを用いる。またVDEは、自由に利用可能な情報（例えば、コンテンツの要旨、表）および制御情報の性能を保証する安全化されコンテンツ制御情報の両方を保持してもよい。コンテンツ制御情報は、オブジェクトのコンテンツに対する権利の保持者によって設定される規格に従って、および／またはそのようなコンテンツの配布に関連する権利を有するパーティ（行政機関、金融クレジットプロバイダ、およびユーザ）に従って、コンテンツ使用を決定する。

一部には、オブジェクトを保護するために用いられる暗号化スキームは改変から関連づけられたコンテンツ制御情報（ソフトウェア制御情報および関連するデータ）を保護するために効率的にさらに用いられ得るので、本発明によって用いられるオブジェクト方法によってセキュリティが高まる。コンテンツの形態での電子情報が（例えば、同一のオブジェクトコンテナ内でコンテンツ情報として）

コンテンツ制御情報と共に挿入され、それによって（前記コンテンツについての）「発行された(published)」オブジェクトを生成させ得るので、このオブジェクト技術によって、様々なコンピュータおよび／または別の機器環境間での移植可能性が高まる。その結果、制御情報の様々な部分は、様々なコンピュータプラットフォームおよびオペレーティングシステムなどの異なる環境に特に適合され得る。様々な部分はすべて、VDEコンテナに搭載され得る。

VDEの目的は、取引／配布制御規格をサポートすることである。そのような規格の発展には、多くの障害、与えられたセキュリティ要件および関連するハードウェアおよび通信問題、非常に異なる環境、情報タイプ、情報使用のタイプ、企業および／またはデータセキュリティ目的、様々な参加者および配送された情報の所有権がある。VDEの重要な特徴は、一部には、電子商取引およびデータセキュリティ機能を安全なハードウェアSPUおよび／または対応するソフトウェアサブシステム内で実行可能な一般化されたケーパビリティモジュールに多くの異なる配布および他の取引変数を分解すること、さらにはVDEインストレーション基

礎上で動作するアプリケーションでのそのようなモジュール（例えば、ロードモジュールおよび／またはメソッド）の組立、改変および／または置換において大きいフレキシビリティを可能にすることによって、多くの様々な配布および他の取引変数を含む。この構成性および再構成性によって、電子商取引およびデータセキュリティ参加者が、発展する拡張された電子契約（電子制御モデル）を反復して適合させるプロセスによってそれらの優先度および要件を反映させ得る。この適合化は、１つのVDE参加者から別の参加者へのコンテンツ制御情報受け渡しとして、「インプレース（in place）」コンテンツ制御情報によって可能になる範囲で生じ得る。このプロセスによって、VDEのユーザは既存の制御情報を再構成(recast)し、および／または必要に応じて新しい制御情報を追加すること（もはや必要のないエレメントを除去することを含む）が可能になる。

VDEは、商業的な電子コンテンツ分散およびデータセキュリティアプリケーションのための信用のある（十分に安全な）電子情報配布および使用制御モデルをサポートする。VDEは、コンテンツクリエータ、コンテンツ配布者、クライアント管理者、エンドユーザおよび／または情報交換所および／または他のコンテンツ使用情報ユーザを含み得る相互に関連する参加者のネットワークの様々な要件を満たすように構成され得る。これらのパーティは、電子コンテンツ配布、使用制御、使用報告および／または使用支払いの単純なものから複雑なものまでに関わる参加者ネットワークを構成し得る。配布されたコンテンツは、元々供給された情報およびVDE生成情報（コンテンツ使用情報など）の両方を含み得、コンテンツ制御情報は、コンテンツおよびコンテンツ制御情報取扱いのチェーン（１つ以上の経路）およびコンテンツの直接の使用の両方を介して持続し得る。本発明によって提供される構成性は、企業が関係を作り、競合する価値を提供する戦略を発展させることを可能にする電子取引をサポートするために特に重要である。本質的に構成可能でも相互動作可能でもない電子取引ツールは、基本的な要件および大半の取引アプリケーションの発展する要求の両方を満たす製品（およびサービス）を最終的に製造し得ない。

VDEの基本的な構成性によって、幅広い範囲の競合する電子商取引企業モデル

が成功し得る。これによって、歳入源、エンドユーザ製品価値、および動作効率を最大化するように企業モデルが適合され得る。VDEは、複数の異なるモデルをサポートするため、新しい歳入機会を利用するため、およびユーザによって最も望まれる製品構成を配送するために用いられ得る。本発明が行う以下の事、すなわち、

！　広範囲の可能な相補的歳入活動のサポート、

！　顧客によって最も望まれるコンテンツ使用特徴のフレキシブルなアレイの提供、および、

！　効率を上げるための機会の利用、

を行わない電子商取引技術を用いると、しばしばより本質的にコストが高く、魅力に乏しく、従って、市場での競合性が低い製品になる。

本発明に本質的な構成性に貢献するキーファクタには、以下が含まれる。

（ａ）システムセキュリティ全体を維持しながら、ほぼすべての電子機器環境における制御および監査ケーパビリティの併合(merging)を効率的にサポートする移植可能APIおよびプログラミング言語ツールを介する、広範な電子機器の基礎的な制御環境への統合；

（ｂ）モジュラーデータ構造；

（ｃ）包括的なコンテンツモデル；

（ｄ）基礎アーキテクチャ構成要素の一般的なモジュール性および独立性；

（ｅ）モジュラーセキュリティ構造；

（ｆ）可変長および制御の複数の分岐チェーン；および

（ｇ）１つ以上のライブラリ中に維持され得、コントロールメソッドおよびモデルに組立てられ得る、実行可能なロードモジュールの形態の独立したモジュラー制御構造であり、制御情報がVDEコンテンツ制御情報取扱いの経路の参加者のVDEインストレーションを通過すると、そのようなモデル制御スキームは「発展」し得る。

本発明によって解決される問題に幅があるために、非常に広範な商業およびデータセキュリティモデルのために、秘匿のおよび／または所有権情報および商業

電子取引の不許可使用を防止し得る単一の取引／配布制御システムを、新たに生じた（emerging）「電子ハイウエイ」に備え得る。VDEの電子取引管理メカニズムは、非常に様々な企業およびデータセキュリティモデルに参加するすべてのパーティの電子権利および契約を実行し得、各VDE参加者の電子機器内の単一のVDEインストレーションによって有効に達成され得る。VDEは、VDEコンテンツおよび／または取扱いのコンテンツ制御情報経路の様々な「レベル」で幅広い参加者を伴い得る、非常に様々な企業および／またはデータセキュリティモデルをサポートする。異なるコンテンツ制御および／または監査モデルおよび契約は、同一のVDEインストレーションで利用可能になり得る。これらのモデルおよび契約は、例えば、一般のVDEインストレーションおよび／またはユーザ、ある特定のユーザ、インストレーション、クラスおよび／またはインストレーションおよび／またはユーザののの他のグループ分けに関するコンテンツ、ならびに広く所与のインストレーション上にある電子コンテンツ、特定の特性、特性部分、クラスおよび／またはコンテンツの他のグループ分けに関するコンテンツを制御し得る。

VDEを用いる配布は、電子コンテンツおよび制御情報の両方を同一のVDEコンテナにパッケージし、および／または複数の別々の遠隔位置からおよび／または複数の別々のVDEコンテンツコンテナにおいておよび／または複数の異なる配送主端を用いて同一のVDE管理特性の異なる部分のエンドユーザサイトへの送達を伴い得る。コンテンツ制御情報は、関連づけられたコンテンツから１つ以上のVDE管理オブジェクト中でのユーザVDEインストレーションへ一部あるいは全体が別々に配送され得る。上記制御情報の部分は、１つ以上の供給源から配送され得る。制御情報は、使用のためにユーザのVDEインストレーション安全サブシステムから１つ以上の遠隔VDE安全サブシステムおよび／またはVDE互換性の認定された安全遠隔位置へのアクセスによって利用可能になり得る。計量、予算作成、復号化および／指紋刻印などのVDE制御プロセスは、あるユーザコンテンツ使用活動に関連するように、ユーザの遠隔VDEインストレーション安全サブシステムにおいて行われても、同一のユーザVDEインストレーションおよび／またはネットワークサーバおよびユーザインストレーション内に配置され得る複数の安全なサブ

システムに分割され得る。例えば、遠隔VDEインストレーションは、復号化および関連する使用計量情報のいずれかまたはすべての保存を行い得、および／またはそのようなユーザインストレーションにおける電子機器使用は、上記の安全なサブシステム間で安全な（例えば、暗号化された）通信を用いるサーバで行われ得る。上記のサーバ位置は、上記のユーザインストレーションからのコンテンツ使用情報のほぼリアルタイムの頻繁な、またはより定期的な安全な受け取りのために用いられ得、例えば、計量された情報は、遠隔ユーザインストレーションでは一時的にのみ維持されている。

VDE管理コンテンツのための送達手段は、上記情報の一部を送達および放送するための光ディスク電子データ格納手段および／または上記の情報の他の部分のための遠隔通信手段などの電子データ格納手段を含み得る。電子データ格納手段は、磁気媒体、光媒体、光磁気システムの組み合わせ、フラッシュRAMメモリ、バブルメモリおよび／またはホログラフィ、周波数および／または極性データ格納技術を用いた大容量光学格納システムなどの他のメモリ格納手段を含む。データ格納手段は、それ自体は単一の厚いディスクとしてまとめて物理的にパッケージされるデータ保持ディスクの層を通って光を通過させる、概して透明および／またはトランスルーセントな材料多層ディスク技術を用いてもよい。そのようなディスク上のデータ保持位置は、少なくとも一部が不透明であり得る。

VDEは、使用制御、監査、報告および／または支払いを含む安全な取引管理のための汎用基礎をサポートする。この汎用基礎は「VDE機能」（「VDEF」）と称される。VDEはまた、選択的に集められ、VDEFアプリケーションおよびオペレーティングシステム機能として働く様々なVDEFケーパビリティ（コントロールメソッドと称される）を形成し得る「原子サイズの」アプリケーションエレメント（例えば、ロードモジュール）の収集もサポートする。電子機器のホスト動作環境がVDEFケーパビリティを含むときは、「権利オペレーティングシステム」（ROS）と称される。VDEFロードモジュール、関連するデータおよびメソッドは、本発明の目的については「制御情報」と称される情報の主要部を形成する。VDEF制御情報は、電子コンテンツの１つ以上の部分と特に関連づけられても、VDEインスト

レーションのオペレーティングシステムケーパビリティの通常の構成要素として用いられてもよい。

VDEF取引制御エレメントは、コンテンツに特定のおよび／またはより一般化された管理（例えば、一般的なオペレーティングシステム）制御情報を反映および規定する。特定のケーパビリティを用いるための、例えば、VDEテンプレートを使用してVDE参加者によって適合化され得る構成性を多少有するアプリケーション（アプリケーションモデル）の形態を概してとり得るVDEFケーパビリティは、例えば、１つ以上のエレメントを反映するためのケーパビリティパラメータデータと共に、市販されている商品などの電子コンテンツの使用に関してVDE参加者間の電子契約を表す。これらの制御ケーパビリティは、電子コンテンツの使用および／または使用の監査、およびコンテンツ使用に基づく報告情報、ならびにその使用に対するいずれもの支払いを管理する。VDEFケーパビリティは、制御情報の与えられたセットを受け取るか、もしくはそのセットに寄与する１つ以上の連続するパーティの要件を反映するために「発展」し得る。与えられたコンテンツモデル（CD－ROM上での娯楽の配布、インターネット容器、または電子カタログショッピングおよび広告、あるいは上記の組み合わせのいくつかなど）のためのVDEアプリケーションについては、しばしば、参加者は、利用可能な代替的なコントロールメソッドを選択し、関連するパラメータデータを与え得る。この場合、このようなコントロールメソッドの選択および／またはデータの提出(submissi

on)は、制御情報の「寄与」を構成する。あるいは（または、そのうえ）、上記のアプリケーションと安全に相互動作可能で互換性があると明確に認定されているあるコントロールメソッドは、そのような寄与の一部として参加者によって独立して提出され得る。最も一般的な例において、概して認定されたロードモジュール（与えられたVDE構成および／またはコンテンツクラスについて認定されている）は、その構成のノードにおいて動作する多くのあるいはいずれものVDEアプリケーションと共に用いられ得る。これらのパーティは、許可される範囲で、ロードモジュールおよびメソッドの仕様を独立して安全に付加、削除、および／

または改変すると共に、関連する情報を付加、削除および改変し得る。

通常、VDEコンテンツコンテナを製作するパーティは、ある電子情報に適用するおよび／または適用し得るVDEFケーパビリティの一般的な性質を規定する。VDEコンテンツコンテナは、コンテンツ（例えば、コンピュータソフトウェアプログラム、映画、電子刊行物、または参考資料などの市販の電子情報）およびオブジェクトのコンテンツの使用に関連するある制御情報の両方を含むオブジェクトである。製作するパーティは、VDEコンテナを他のパーティに利用可能にし得る。VDEコンテンツコンテナによって配送され、および／またはVDEコンテンツコンテナを用いた使用について利用可能な制御情報は、（コンテンツ市販のために）電子コンテンツのためのVDEF制御ケーパビリティ（およびいずれもの関連するパラメータデータ）を含む。これらのケーパビリティは、そのようなコンテンツの使用および／または使用の結果を管理し、複数のパーティに関連する約定および条件ならびにそれらのパーティの様々な権利および義務を規定し得る１つ以上の「提案される」電子契約（および／またはパラメータデータの選択および／または使用のために利用可能な契約機能）を構成し得る。

VDE電子契約は、１つ以上のパーティー－例えば、「上位の」パーティから制御情報を受けとった「下位の」パーティー－によるユーザインタフェース受領によって明らかにされてもよいし、また、自分自身の契約を個々に主張する同等のパーティ間のプロセスであってもよい。契約は、コンテンツに付加されているおよび／または別のパーティによって提出されているある別の電子約定および条件が許容可能か（許容可能な制御情報基準に違反していないか）を判断するあるVDE参加者制御情報によって約定および条件が「評価される」、自動化電子プロセスから生じてもよい。そのような評価プロセスは非常に単純なプロセス、例えば、約定および条件のテーブル内での制御約定および条件の一部またはすべての上位制御約定および条件と、コンテンツ制御情報取扱いの経路における次の参加者の提出された制御情報との間の互換性を保証するための比較などであっても、２つ以上のパーティによって提出される２つ以上の制御情報のセット間の交渉プロセスの潜在的な結果を評価および／または交渉プロセスを実行するより複雑なプ

ロセスであってもよい。VDEはまた、１つ以上の他のパーティの利益および／または別の選択肢の選択および／またはあるパラメータ情報のためのあるユーザインタフェース問い合わせに対する回答を表す制御情報に対して許容可能であり得るある制御情報を許容および／または提案することによってユーザインタフェース手段により１つ以上のVDE参加者が制御情報セット間の「不一致」を決定する、半自動化プロセスを含む。ここで、応答は、適用可能な上位の制御情報に許容可能である場合に適合される。

別のパーティ（最初の規則適用者以外）が、おそらくは交渉プロセスを介して、「インプレース」コンテンツ制御情報を受け取り、および／または制御情報に付加し、および／または改変すると、そのような電子コンテンツの使用に関連する２つ以上のパーティ間のVDE契約が（いずれもの改変が上位の制御情報と一致する限り）行われ得る。ある電子コンテンツに関連する約定および条件の許容は直接的で明確であっても、（例えば、法的要件、そのような約定および条件を前もって与えること、および適切な制御情報の要件に依存した）コンテンツの使用の結果として暗示的（implicit）であってもよい。

VDEFケーパビリティをある特定の電子情報の制御と直接関連付けずに複数のパーティによってVDEFケーパビリティが用いられても、VDE契約が行われてもよい。例えば、VDEインストレーションにおいてある一つ以上のVDEFケーパビリティが存在してもよく、VDEコンテンツ使用の安全な制御、監査、報告および／または支払いのためのそのようなインストレーションによって使用されるために、コンテンツ配布アプリケーションのための登録プロセスの間に、あるVDE契約が行われてもよい。同様に、ユーザおよび／またはその機器がVDEインストレーション

および／またはユーザとしてそのようなプロバイダに登録するときに、特定のVDE参加者はVDEコンテンツまたは電子機器プロバイダとVDEユーザ契約を行い得る。そのような場合には、ユーザVDEインストレーションに利用可能なVDEFに適した制御情報は、電子コンテンツおよび／またはVDEアプリケーションのすべておよび／またはいくつかのクラスを使用し得るようにするために、例えば、あるシ

ーケンスにおいていくつかのVDEFメソッドが用いられることを必要とし得る。

VDEによって、与えられた取引に必要なある必須条件が安全に満たされる。これは、いずれもの必要とされるモジュールの安全な実行およびいずれもの必要とされる関連づけられたデータが利用可能であることを含む。例えば、（メソッドの形態などでの）必要とされるロードモジュールおよびデータは、許可された供給源からの十分なクレジットが利用可能であると確認されなければならないことを指定し得る。これは、そのようなクレジットがコンテンツのユーザの使用に対する支払いを行うために安全に用いられるようにするために、適切な時間でのプロセスとしてある一つ以上のロードモジュールを実行することをさらに必要とし得る。あるコンテンツプロバイダは、例えば、与えられたソフトウェアプログラム（プログラムの一部は暗号化された形態で維持され、実行のためにはVDEインストレーションが存在することを必要とし得る）の使用者への配布のために行われるコピー部数を計量することを必要とし得る。これには、別の使用者に対してコピーが作られるたびに、プロバティのコピーのための計量法を実行することを必要とする。この同一のプロバイダはまた、ユーザによってプロバティから認可された異なるプロバティの合計数に基づいて料金を請求し、プロバティの認可の計量履歴がこの情報を維持するために必要になり得る。

VDEは、組織、共同体および／またはVDE参加者ユーザインストレーション（ノード）において安全に制御されるプロセスによって保証される統合性を有する世界規模の安全な環境を提供する。好ましい実施態様において、VDEインストレーションは、ソフトウェアおよび不正改変不可能なハードウェア半導体素子の両方を含み得る。そのような半導体構造は、VDEの制御機能を行う際に用いられる情報および機能を用いる不正改変あるいはその不許可観測を防止するように設計された特殊目的回路を、少なくとも一部が備えている。本発明による、特殊目的安全回路は、安全処理ユニット（SPU）として知られている専用半導体構成および／または標準マイクロプロセッサ、マイクロコントローラ、および／または本発明の要件を満たし、SPUとして機能する別の処理論理の少なくとも一つを含む。VDEの安全ハードウェアは、例えば、ファックス／モデムチップまたはチップパッ

ク、I/Oコントローラ、映像表示コントローラ、および／または別の利用可能なディジタル処理構成に組み込まれることが見出され得る。本発明のVDE安全ハードウェアケーパビリティの一部は、最終的には、コンピュータおよび他の様々な電子処理装置のための中央処理装置（CPU）の標準設計装置になり得ることが予期される。

VDEケーパビリティを１つ以上の標準マイクロプロセッサ、マイクロコントローラおよび／または他のディジタル処理コンポーネント内に設計することにより、本発明によって考慮される取引管理使用および他のホスト電子機器機能の両方について同一のハードウェアリソースを用いることができ、それによって、材料面においてVDE関連ハードウェアコストを下げ得る。これは、VDE SPUは、「標準」CPUの回路素子を用い（共有）し得ることを意味している。例えば、「標準」プロセッサが保護モードで動作し、VDE関連命令を保護下の活動として実行し得る場合、そのような実施の形態は様々なアプリケーションについて十分なハードウェアセキュリティを提供し、特殊目的プロセッサの出費が抑えられ得る。本発明の１つの好ましい実施の形態では、あるメモリ（例えば、RAM、ROM、NVRAM）は、保護モードで（例えば、保護モードマイクロプロセッサによってサポートされるように）VDE関連命令処理の間に維持される。このメモリは、処理論理（例えば、プロセッサ）として同一パッケージ内に配置される。望ましくは、そのようなプロセッサのパッケージングおよびメモリは、耐不正改変性を高めるセキュリティ技術を用いて設計される。

VDEシステム全体のセキュリティの程度は、耐不正改変性およびVDE制御プロセス実行および関連するデータ格納活動の隠蔽の程度に主に依存する。特殊目的半導体パッケージ技術の使用は、セキュリティの程度に非常に寄与し得る。半導体メモリ（例えば、RAM、ROM、NVRAM）における隠蔽および耐不正改変性は、そのようなメモリをSPUパッケージ内で用い、データが外付けメモリ（外付けRAMパッケージなど）に送られる前にデータを暗号化し、暗号化されたデータが実行される前に暗号化されたデータをCPU／RAMパッケージ内で復号化することによって、一部が達成され得る。このプロセスは、このようなデータが保護されない媒体、

例えば、ランダムアクセスメモリ、大容量記憶装置などの標準ホスト記憶装置に格納されるとき、重要なVDE関連データのために用いられる。このような場合、VDE SPUは、そのようなデータが外付けメモリに格納される前に安全なVDE実行から得られるデータを暗号化する。

本発明によるVDEによって提供される重要な一部の特徴の概要

VDEは、汎用の、十分に安全な分散型電子取引解決法のための基礎となる様々なケーパビリティを用いる。VDEによって、散在する、競合する企業提携、契約および発展する全体的な企業モデルをサポートする電子取引市場が可能になる。例えば、VDEは、以下の特徴を有する。

安全な通信、格納および取引管理技術による、電子情報および／または機器の非許可および／または補償されない使用の「十分な」防止。VDEは、単一の安全な「仮想」取引処理および情報格納環境を形成するモデルワイド（model wide）の分散型のセキュリティ実施をサポートする。VDEによって、分散型のVDE実施が、情報を安全に格納および通信し、別のVDE実施において幅広い方法で実施プロセスおよび電子情報の使用の特徴を遠隔に制御することが可能になる。

！　取引制御、監査、報告および関連する通信および情報格納のための低コストの効率的で有効なセキュリティアーキテクチャをサポートする。VDEは、タグ付けに関連するセキュリティ技術、暗号化鍵のエージング、格納された制御情報（置換および不正改変に対する保護を行うためのそのような情報の差動(differentially)タグ付けを含む）および配布されたコンテンツ（多くのコンテンツアプリケーションについて、特定のVDEインストレーションおよび／またはユーザに独特の1つ以上のコンテンツ暗号化鍵を用いるため）の両方の区分化、コンテンツを暗号化するためのトリプルDESなどの暗号鍵技術、通信を保護し、ディジタル署名および認証の利点を与え、それによってVDE構成のノードを互いに安全に結合させるＲＳＡなどの公開鍵技術、重要な取引管理実行可能コードの安全な処理、および少量の非常に安全なハードウェア保護記憶スペースと安全化された（通常は暗号化およびタグ付けされている）制御および監査情報を格納するより大きな「露出された(exposed)」マスメディア格納スペースとの組み合わせを用

い得る。VDEは、VDE実施の一部あるいはすべての位置に配布されている特殊目的ハードウェアを用いている。ａ）上記ハードウェアは、コンテンツ準備（そのようなコンテンツをVDEコンテンツコンテナ内に配置し、コンテンツ制御情報をそのコンテンツと関連づけるなど）、コンテンツおよび／または電子機器使用監査、コンテンツ使用分析、ならびにコンテンツ使用制御の重要な要素を制御し、ｂ）上記ハードウェアは、処理ロードモジュール制御活動を安全に取り扱うように設計され、この制御処理活動は必要とされている制御要因のシーケンスを伴い得る。

！　VDE電子情報製品（VDE制御されたコンテンツ）の情報サブセットの動的なユーザ選択をサポートする。これは、そのような製品あるいはセクションの一部を得るためまたは用いるために情報製品全体または製品セクションを選択することが必要となるようないくつかの高レベルの個別の前もって規定されたコンテンツプロバイダ情報インクリメントを用いなければならない制約と対照をなす。VDEは、形成するユーザによってそのためだけに選択され、概して任意であるが、ユーザにとって論理的コンテンツを「配送可能」にする前もって識別された１つ以上のインクリメント（例えば、バイト、イメージ、論理に関連づけられたブロックなどの前もって識別された性質を有する１つ以上のブロックなど）が収集されたものを表す様々なインクリメント（「原子的」インクリメント、および異なるインクリメントタイプの組み合わせを含む）への計量および使用制御をサポートする。VDE制御情報（予算作成、価格決定および計量を含む）は、情報インクリメントの異なる予期されない可変的ユーザ選択の集積のそのためだけの選択に、適切なように特定的に適用され得るように、かつ、価格決定レベルが、少なくとも一部が、混合されたインクリメント選択の量および／または性質（例えば、ある量のあるテキストの、関連づけられたイメージが１５％割引され得ることを意味し、「混合」インクリメント選択におけるより多い量のテキストは、イメージが２０％割引され得ることを意味する）に基づき得るように構成され得る。このようなユーザ選択の集積情報インクリメントは、情報についてのユーザの実際の要件

を反映し得、単一の、またはいくつかの高レベルの（例えば、製品、文書、データベース記録）所定インクリメントに限定されるものよりもフレキシブルである。そのような高レベルインクリメントは、ユーザによって望まれない量の情報を含み、その結果、サブセットが利用可能である場合にユーザが必要とする情報のサブセットよりもよりコストが高くなり得る。要するに、本発明によって電子情報製品に含まれている情報をユーザ仕様に従って供給することが可能になる。ユーザ仕様に適合することによって、本発明はユーザに最大の価値を与えることが可能になり、そのことによって最大量の電子取引活動が生じる。ユーザは、例えば、入手可能なコンテンツ製品の様々な部分から得られるコンテンツの集積を規定し得るが、これらの部分は、ユーザによる使用のために配送可能なものとして、完全に独特の集積インクリメントである。ユーザは、例えば、参考資料などの情報製品の様々な部分からの情報のある数のバイトを選択し、それらのバイトを非暗号化形態でディスクにコピーし、バイトの総数に加えてそのバイトを提供した「商品」の数に対する追加金に基づいて課金され得る。ユーザは、所望の情報を含むすべての商品からのすべてのコンテンツは必要としていないので、コンテンツプロバイダは、そのようなユーザ規定情報インクリメントについては合理的にはより低い金額を請求され得る。ユーザが所望とする情報インクリメントを規定するこのプロセスは、情報製品からの情報の最も関連する部分の位置に寄与し、ユーザ選択またはそのような部分のユーザへの自動的な抽出および配送のためのサーチ基準ヒットを示す情報のユーザに自動的な表示を行う、人工的知能データベースサーチツールを含み得る。VDEは、以下を含む非常に様々な前もって規定されているインクリメントタイプをさらにサポートする。

！バイト、

！イメージ、

！音声または映像のための経時的コンテンツ、または

！文、

！段落、

！章

！データベース記録、および

！論理的に関連づけられた情報のインクリメントを表すバイトオフセットなどのコンテンツプロバイダデータマッピング労力によって識別され得る他のいずれものインクリメント。

VDEは、与えられたタイプのコンテンツおよび企業モデルについて実用的であり得る数と同じ数の、前もって規定された同時のインクリメントタイプをサポートする。

！　暗号化データ形態で詳細な情報を維持するため、かつ、非常に安全な特殊目的VDEインストレーション不揮発性メモリ（利用可能である場合）でセキュリティテストのために概要情報を維持するための安価な「露出」ホスト大容量記憶装置を用い、様々な異なるコンテンツセグメントタイプのユーザの使用を反映する潜在的に非常に詳細な情報をユーザの位置に安全に格納する。

！　配布された電子情報の経路および／またはコンテンツ使用関連情報のための取扱いケーパビリティの信用されたチェーンをサポートする。このようなチェーンは、例えば、コンテンツクリエータから配布者、再配布者、クライアントユーザに拡張し、次いで、同一のおよび／または異なる使用情報を、１つ以上の独立した情報交換所などの１つ以上の監査者に安全に報告し、次いで、コンテンツクリエータを含むコンテンツプロバイダに戻すための経路を提供し得る。あるコンテンツ取扱い、関連する制御情報および報告情報取扱いのために用いられる同一および／または異なる経路は、電子コンテンツおよび／または機器仕様のための電子支払い処理（本発明において支払いは管理コンテンツとして特徴づけられる）のための１つ以上の経路としても用いられ得る。これらの経路は、コンテンツ全体および一部および／またはコンテンツ関連制御情報の搬送に用いられる。コンテンツクリエータおよび他のプロバイダは、商業的に配布されるプロパティコンテンツ、コンテンツ制御情報、支払い管理コンテンツ、および／または関連する使用報告情報を配信するために一部あるいは全体が用いられなければならない経路を指定し得る。コンテンツプロバイダによって指定される制御情報は、特定のパーティが運搬された情報を取り扱わなければならないあるいは取扱い得る（例えば、選択が行われ得る適当なパーティのグループを含む）ものを指定し得る。これはまた、どの伝達手段（例えば、遠隔通信キャリアあるいは媒体タイ

プ）および伝達ハブが用いられなければならないあるいは用いられ得るかを指定し得る。

！　高い効率の動作およびスループットを達成し、それまでの使用活動に関連する情報および関連するパターンの保持および実行可能なリコールを実用的な方法で可能にする「ビットマップ計量」を用いるなどのフレキシブルな監査メカニズムをサポートする。このフレキシブルさは、非常に様々な以下の課金およびセキュリティ制御戦略に適合可能である。

P　アップグレード価格設定（例えば、継続購入）、

P　価格割引（量による割引を含む）、

P　過去の購入のタイミングに基づく新たな購入の割引などの課金関連期間変数、および

P　ある時間間隔にわたって用いられる電子情報の異なる、論理に関連するユニットの量に基づくセキュリティ予算。

本発明の好ましい実施の形態の他の要素と共に情報の使用および／購入を記録するためのビットマップ計量（「正規」および「ワイド」ビットマップ計量を含む）の使用は、（ａ）レンタル、（ｂ）均一料金ライセンス認可あるいは購入、（ｃ）履歴使用変数に基づくライセンス認可または購入の割引、および（ｄ）あるアイテムが獲得されたかあるいはある期間内に獲得されたかを（これらのアプリケーションについては非常に非効率的な従来のデータベースメカニズムの使用を必要とせずに）決定することをユーザに可能にするようにユーザへ報告を行うこと、についての使用履歴の効率的な維持を一義的にサポートする。ビットマップ計量法は、コンテンツおよび／または機器プロバイダおよび／または管理活動のコントローラが過去のいくつかの時点あるいはある期間の間（例えば、商業的電子コンテンツ製品および／または機器）にある活動が生じたかを決定し得るように、ユーザおよび／または電子機器によって行われる、特定の特性、オブジェクトなどとは無関係の電子機器、特性、オブジェクト、またはそれらの一部、および／または管理と関連する活動を記録する。次いで、そのような決定は、コンテンツおよび／または機器プロバイダの価格決定および／制御戦略の一部、および／または管理活動のコントローラとして用いられ得る。例えば、コンテンツプ

ロバイダは、プロパティの一部がユーザによってアクセスされる回数とは無関係に、プロパティの一部へのアクセスに対して１度のみ課金することを選択し得る。

！　コンテンツプロバイダによってエンドユーザに供給され得るコンテンツである「ランチ可能な（launchable）」コンテンツをサポートすることであり、エンドユーザは、次いで使用のためのコンテンツを登録および／または初期化するためにコンテンツプロバイダが直接参加することを必要とせずに、コンテンツを別のエンドユーザパーティにコピーするかあるいは受け渡し得る。このコンテンツは、「移動オブジェクト(traveling object)」の形態で「（従来の配布）チャネル外」で進む。移動オブジェクトは、少なくともいくつかのパーミッション情報および／または使用のために必要とされるメソッド（そのようなメソッドは、必要とされるメソッドが、目的地VDEインストレーションにおいて利用可能、あるいは目的地VDEインストレーションに対して直接利用可能である場合は、移動オブジェクトによって運ばれる必要はない）を安全に運ぶコンテナである。ある移動オブジェクトは、所与のVDE構成の一部またはすべてのVDEインストレーションの一部またはすべてにおいて用いられ得る。なぜなら、商業的なVDE価値チェーン参加者またはデータセキュリティ管理者（例えば、制御員あるいはネットワーク管理者）が関わることを必要とせずにコンテンツ使用に必要なコンテンツ制御情報を利用可能にし得るからである。移動オブジェクトの制御情報要件がユーザVDEインストレーション安全サブシステム（承認されたクレジットプロバイダからの十分な量の金融クレジットがあることなど）で利用可能である限り、少なくともいくつかの移動オブジェクトコンテンツは、遠隔VDE権限との関係を確立する必要なしに、受け取りパーティによって用いられ得る（例えば、予算が使い尽くされるか、あるいは時間コンテンツ使用報告間隔が生じるまで）。移動オブジェクトは、「チャネル外で」移動し、ユーザが、例えば、コンテンツがソフトウェアプログラム、映画、またはゲームである移動オブジェクトのコピーを近隣者に与えることを可能にする。近隣者は、適切なクレジット（例えば、VISAあるいはAT&Tなどの情報交換所からの情報交換所アカウント）が利用可能である場合、移動オブジェクトを用いることができる。同様に、インターネット上（あるいは

類似のネットワーク）の格納場所で一般的に入手可能な電子情報は、ダウンロードされ、次いで初期のダウンロード者によってコピーされ、オブジェクトを付加的なパーティに受け渡し得る他のパーティに受け渡され得る移動オブジェクトの形態で提供され得る。

！　個人、インストレーション、クラスなどのグループ、ならびに機能およびクライアント識別（例えば、クライアント識別ＩＤ、クライアント部門ＩＤ、クライアントネットワークＩＤ、クライアントプロジェクトＩＤ、およびクライアント雇用者ＩＤ、あるいはいずれもの上記の適切なサブセット）のレベルの階層を用いた階層識別による、非常にフレキシブルで拡張可能なユーザ識別を提供する。

！　取引制御および監査のために製作された実行可能なコード部分を用いる基礎取引オペレーティングシステム環境として機能する汎用の安全なコンポーネントベースのコンテンツ制御および配布システムを提供する。これらのコード部分は、信用される分散型の取引管理構成の形成および動作における効率を最適化するために再利用され得る。ＶＤＥは、「原子的」ロードモジュールおよび関連づけられたデータの形態のそのような実行可能なコードの提供をサポートする。多くのそのようなロードモジュールは、本質的に構成可能、集積可能、移植可能、拡張可能であり、単一であるいは組み合わせられて（関連づけられたデータと共に）、ＶＤＥ取引動作環境下でコントロールメソッドとして実行される。ＶＤＥは非常に異なる電子取引およびデータセキュリティアプリケーションの要件を、一部には、ＶＤＥ取引関連コントロールメソッドを安全に処理するためにこの汎用取引管理基礎を用いることによって満たし得る。コントロールメソッドは、主に、一つ以上の上記の実行可能な再利用可能なロードモジュールコード部分（通常は、実行可能なオブジェクトコンポーネントの形態である）および関連付けられたデータの使用によって形成される。コントロールメソッドのコンポーネント性質によって、本発明が高度に構成可能なコンテンツ制御システムとして効率的に動作することが可能になる。本発明では、コンテンツ制御モデルは、もし行われる場合（新しいコンポーネントアセンブリが許容されるか、もし許容される場合、認定要件がそのようなコンポーネントアセンブリに対して存在するか、あるいはいずれか

のあるいはある参加者が選択的な制御情報（パーミッション記録）コントロールメソッドからの選択によっていずれかのあるいはある制御情報を適合化し得るか）。

そのような適合および更新がVDEアプリケーションによって与えられる制約に合う程度にVDE参加者の要求を満たすように反復的および非同期的に適合化されるか、更新され得る。この反復的な（または同時の）複数参加者プロセスは、安全な制御情報コンポーネント（ロードモジュールおよび／またはメソッド、および／または関連するデータなどの実行可能なコード）の提出および使用の結果として生じる。これらのコンポーネントは、VDE参加者のVDEインストレーションに影響を与える各制御情報間の安全な通信によって独立して与えられ得、与えられたアプリケーションとともに用いるための証明を必要とし得、この場合そのような証明は、機器および提示されるコントロールメソッド間の安全な相互動作性および／信頼性（例えば、相互作用から得られるバグ制御）を確実にするVDE構成のための証明サービスマネージャによって与えられる。VDE電子機器取引動作環境の取引管理制御機能は、安全ではない取引管理オペレーティングシステム機能とインタラクトし、それによって取引プロセスおよび電子情報セキュリティ、使用制御、監査および使用報告に関連するデータを適切に導く。VDEは、安全なVDEコンテンツおよび／または機器制御情報実行およびデータ格納に関連するリソースを管理するためのケーパビリティを提供する。

！　VDE下のアプリケーションおよび／またはシステム機能性の形成を促進し、本発明によって形成されたロードモジュールおよびメソッドの電子機器環境への統合を促進する。これを達成するためには、VDEはアプリケーションプログラマのインタフェース（API）および／または組み込み関数をもつ取引オペレーティングシステム（ROSなど）プログラミング言語を用いる。これらは両方とも、ケーパビリティの使用をサポートし、VDE機能性を商業的およびユーザアプリケーションに効率的かつしっかりと統合するために用いられ得る。

！　（ａ）例えば、ユーザにメッセージを与え、取引の認可などの特定の行動をユーザが取り得るようにするための「ポップアップ」アプリーション、（ｂ）取

引毎、時間ユニット毎および／またはセッション毎の価格を制限するため、前の取引に関する履歴情報にアクセスするため、予算、消費（例えば、詳細なおよび／または大まかな）および使用分析情報を再検討するためのエンドユーザ嗜好仕様などのユーザ活動に管理環境を提供するスタンドアロンVDEアプリケーション

、

および（ｃ）基礎となる機能性は商業的なソフトウェアの元の設計に組み込まれるので、VDEユーザ制御情報およびサービスはそのようなソフトウェアに継ぎ目なく組み込まれ、ユーザによって直接アクセスされ得るように、VDE「認識」を商業的または内部ソフトウェア（アプリケーションプログラム、ゲームなど）を、VDE APIおよび／または取引管理（例えば、ROSベースの）プログラミング言語を使用した結果として埋め込むVDE認識アプリケーションを通してユーザインタラクションをサポートする。例えば、VDE認識ワードプロセッサアプリケーションにおいて、文書をVDEコンテンツコンテナオブジェクトに「印刷」し、異なる目的のための一連の異なるメニューテンプレートから選択することによって（例えば、内部組織目的のための安全なメモテンプレートは、「保持」する能力すなわち、メモの電子コピーを行う能力を制限し得る）特定の制御情報を与えることができ得る。

！　本発明の構成ケーパビリティのプロセスが特定の産業または企業に関連するとき、それらのプロセスを容易にするために「テンプレート」を使用する。テンプレートは、本発明によるとアプリケーションあるいはアプリケーションアドオンである。テンプレートは、特定のコンテンツタイプに関連する効率的な仕様および／または基準に対する操作、配布アプローチ、価格設定メカニズム、コンテンツおよび／または管理活動とのユーザ相互作用などをサポートする。本発明によってサポートされる非常に広範なケーパビリティおよび構成を与えると、与えられた企業モデルに特に適した管理可能なサブセットに対する構成の機会の幅を減少させることによって、複雑なプログラミングおよび／または構成設計責任に負担を感じている「一般的な」ユーザが本発明の全構成可能能力を容易に用いることが可能になり、また、テンプレートアプリケーションは、独立したモジュー

ルおよびアプリケーション間のコード相互作用の予測不可能な側面およびそのようなモジュールにおけるウイルス存在の可能性と関連するセキュリティ危険性を含む、独立して開発されたロードモジュールの寄与に関連する危険性を低減することによって、VDE関連プロセスが安全で最適にはバグがないものであることを確実にし得る。テンプレートを使用することによって、複数の選択肢、アイコン選択、および／またはメソッドパラメータデータ（識別情報、価格、予算制限、

日付、期間、特定のコンテンツへのアクセス権など）のプロンプトなどの制御情報目的のために適切なおよび／または必要なデータを供給するメニュー選択によるメソッドタイプ（例えば、機能性）の選択を含む適切にしぼられた組の活動に対する一般的なユーザ構成責任がVDEにより低減される。そのユーザ、コンテンツまたは他の企業モデルに対応する一般的な要件を反映するために前もって設定された一般的な構成環境（テンプレート）を有する構成活動の制限されたサブセットに一般的な（非プログラミング）ユーザを制限することによって、関連する相互動作性問題（セキュリティ、オペレーティングシステム、および／または証明非互換性から生じる矛盾など）を含む、コンテンツコンテナ化（初期制御情報をコンテンツ上に配置することを含む）、配布、クライアント管理、電子契約実施、エンドユーザ相互作用および情報交換所活動と関連する問題を実質的に大幅に制限し得る。適切なVDEテンプレートを用いることによって、コンテンツVDEコンテナ化、他の制御情報の寄与、通信、暗号化技術および／または鍵などに関連するユーザの活動が、分散型のVDE構成のための仕様に応じることがユーザに保証され得る。VDEテンプレートは、発展するか、発展するときに新しい企業への適合を反映する新しいおよび／または改変されたテンプレートを可能にする、あるいは既存の企業の発展他の変化を反映するために通常は再構成可能であり得る前もって設定された構成を構成する。例えば、テンプレートの概念は、映画、音声記録およびライブパフォーマンス、雑誌、電話ベースの小売り、カタログ、コンピュータソフトウェア、情報データベース、マルチメディア、商業通信、広告、市場観測、情報提供（infomercial）、ゲーム、数により制御される機械のためのCAD/CAMサービス、などを形成、改変、市場で販売、配布、消費および／また

は使用する組織および個人のための個々の枠組み全体を提供するために用いられ得る。これらのテンプレートを取り巻くコンテクストは変化あるいは発展するので、本発明によって提供されるテンプレートアプリケーションは、幅広い仕様のためあるいはよりしぼられた活動のためにこれらの変化に適合するように改変され得る。初期VDEコンテナ中にコンテンツを配置するパーティは、コンテンツのタイプおよび／またはコンテンツに関連する企業モデルに依存して、様々な異なる構成可能なテンプレートを有し得る。エンドユーザは、異なる文書タイプ（eメー

ル、安全な内部文書、データベース記録など）および／または（異なるユーザに制御情報の異なる一般的な組を与える、例えば、ある前もって設定された基準である文書を用い得るユーザのリストを選択する）ユーザのサブセットに適用され得る異なる構成可能なテンプレートを有し得る。ある状況下では、テンプレートは固定された制御情報を有し得、ユーザ選択およびパラメータデータ入力に対して与えなくてもよいことは明らかである。

！　電子情報コンテンツの同一の特定のコピーおよび／または同一の電子情報コンテンツの複数の異なる制御モデルの異なって規制された異なるコピー（発生）のいずれかの使用および／または監査を規制する複数の異なる制御モデルをサポートする。課金、監査およびセキュリティのための異なるモデルは、電子情報コンテンツの同一の部分に適用され得、そのような異なるセットの制御情報は、制御のためには、電子情報制御インクリメントの同一のあるいは異なる細分性を用い得る。これは、様々な異なる予算および／または、計量の課金ユニット、クレジット制限、セキュリティ予算制限およびセキュリティコンテンツ計量インクリメント、および／または市場観測および顧客プロファイリングコンテンツ計量インクリメントのために配送可能な与えられた電子情報のための計量インクリメントを用いることを含む、電子情報の前もって規定された様々なインクリメントに適用されるように、予算作成および監査使用のための可変性使用情報をサポートすることを含む。例えば、科学記事のデータベースを有するCD－ROMディスクは、復号化されたバイト数、復号化されたバイトを含む記事の数に基づく公式に従

って、一部は課金され得るが、セキュリティ予算は、インストールされているワイドエリアネットワーク上のユーザにデータベースの使用を毎月データベースの５％までに制限し得る。

！　コンテンツおよびコンテンツ制御情報の取扱いの十分に安全なチェーンおよびそのようなコンテンツの使用の様々な形態を介する信用されるコンテンツ使用および報告制御情報を持続して維持するためのメカニズムを提供し、制御の持続性によってそのような使用が継続され得る。制御の持続性は、少なくとも一部が安全化されたコンテンツを有し、元のコンテナの情報を制御し、および／またはこの目的のために元のコンテナの制御情報によって少なくとも一部が生成された

抽出されたコンテンツおよび制御情報の少なくとも一部の両方を含む新しいコンテナを作成することによって、VDEコンテナオブジェクトから情報を抽出する能力を含み、および／またはVDEインストレーション制御情報規定は、新たに形成されたコンテナ内のコンテンツの使用を持続および／または制御するべきである。そのような制御情報は、各々が異なる供給源から誘導された（抽出された）コンテンツを含む、複数の埋め込まれたVDEコンテナを含むオブジェクトなどの他のVDE管理オブジェクトにコンテナが「埋め込まれる」場合、コンテナコンテンツの使用を管理し続け得る。

！　ユーザ、他の価値チェーン参加者（情報交換所および行政機関など）および／またはユーザ組織に、電子コンテンツおよび／または機器の使用に関連する嗜好または要件を特定することを可能にする。市販のコンテンツ（ゲーム、情報リソース、ソフトウェアプログラムなど）を用いるエンドユーザ顧客コンテンツユーザなどのコンテンツユーザは、上位の制御情報、予算および／または他の制御情報によって許可された場合、コンテンツのそれ自体の内部使用の管理を規定し得る。使用は、例えば、ユーザ承認を事前に表明せずにユーザが支払いを行いたい電子文書の価格に制限を設定するユーザ、およびユーザが収集されることを許可したい計量情報の特徴を確立するユーザ（プライバシー保護）を含む。これには、VDEインストレーションの使用から得られる情報およびコンテンツおよび／

または機器使用監査のプライバシーを保護するための、コンテンツユーザのための手段を提供することを含む。特に、VDEは、参加者の暗黙のあるいは明示的な契約なしで電子コンテンツの参加者の使用に関連する情報を他のパーティに与えることを防止し得る。

！　少なくとも一部が独立して安全に配送される付加的な制御情報に従って制御情報を「発展」させ、改変することを可能にするメカニズムを提供すること。この制御情報は、特定のVDEアプリケーション、アプリケーションのクラス、および／またはVDE配布構成と共に用いるために許容可能な（例えば、信頼性のある、および信用された）であるとして認定された実行可能なコードを含み得る。制御情報のこの改変（発展）は、制御情報の取扱い経路において一人以上のVDE参加者に循環するコンテンツ制御情報（ロードモジュールおよびいずれもの関連づけ

られたデータ）上で生じ得るか、あるいはVDE参加者から受け取られる制御情報上で生じてもよい。コンテンツ制御情報の取扱いは、各々が承認されている範囲で、電子コンテンツおよび／または機器（例えば、VDE制御特性コンテンツの使用に関連するように）制御、分析、支払いおよび／または報告使用に関連するパーミッション、監査、支払いおよび報告制御情報を確立、改変および／またはそれらに寄与し得る。（認定に関して以外は独立している独立供給源から）独立して配送された、少なくとも一部が安全な制御情報は、コンテンツ制御情報がVDEコンテンツ制御情報取扱いのシーケンス中である一つのパーティから他のパーティに流れるときに、コンテンツ制御情報を安全に改変するために用いられ得る。この改変は、例えば、VDE安全サブシステム中で安全に処理される１つ以上のVDEコンポーネントアセンブリを用いる。別の実施の形態において、通常はVDE管理オブジェクトの形態である「下位」のパーティから提出された少なくとも一部が安全化された制御情報を受け取った後に、VDEインストレーション安全サブシステムを使用して、制御情報は上位のパーティによって改変され得る。VDE経路に沿って通過する制御情報は、制御情報ハンドラのシーケンスを介して持続された制御情報、改変され得る他の制御情報、および新しい制御情報および／または介

在するデータを表す別の制御情報を含み得る点で、混合された制御セットを表し得る。そのような制御セットは、配信されたコンテンツについての制御情報の発展を表す。本実施例において、提案される制御情報が安全に受け取られ取り扱われる新しい参加者のVDEインストレーションに少なくともコンテンツ制御セットの一部が安全に受け渡されるに従って（例えば、暗号化された形態で通信され、認証およびディジタル署名技術を用いて）、VDEコンテンツコンテナのためのコンテンツ制御セット全体は「発展」していく。受け取られた制御情報は、両方の制御情報セットを伴うネゴシエーションプロセスを介して適所にある制御情報と（受け取りを行うパーティのVDEインストレーション安全サブシステムの使用によって）統合され得る。例えば、コンテンツプロバイダのVDEインストレーション内での、あるVDEコンテンツコンテナのためのコンテンツ制御情報の改変は、金融クレジットプロバイダによって提供される要求される制御情報の組み込みの結果として生じ得る。このクレジットプロバイダは、この必要とされる制御情報

を準備し、そのコンテンツプロバイダに（直接的または間接的に）通信するためにVDEインストレーションを用い得る。この必要とされる制御情報の組み込みによって、エンドユーザが金融クレジットプロバイダとクレジットアカウントを有し、そのクレジットアカウントが十分な利用可能なクレジットを有している限り、VDE制御コンテンツおよび／または機器のエンドユーザの使用を保証するためにコンテンツエンドユーザがクレジットプロバイダのクレジットを使用することが可能になる。同様に、税金の支払いを必要とする制御情報および／または電子商取引活動から生じる歳入情報は、コンテンツプロバイダによって安全に受け取られ得る。この制御情報は、例えば、行政機関から受け取られ得る。コンテンツプロバイダは、市販のコンテンツおよび／または機器使用に関連するサービスについての制御情報に、そのような制御情報を組み込む法律によって必要とされ得る。提案される制御情報は、上位の制御情報によって許容される範囲で、各セット（受け取られたセットおよび提案されたセット）によって規定される優先度を満たすいずれものネゴシエーショントレードオフによって決定されるように用いられる。VDEはまた、VDEコンテンツ取扱い参加者のネットワーク内で異なる参加

者（例えば、個人の参加者および／または参加者クラス（タイプ））に特に適合する異なる制御スキームも考慮する。

！　同一のコンテンツプロパティおよび／またはプロパティの部分のための複数の同時的制御モデルをサポートする。これによって、例えば、歳入を増加させ、その結果、ユーザに対するコンテンツコストを下げ、コンテンツプロバイダに対する価値を上げる、詳細な市場観測情報の獲得および／または広告のサポートなどの電子商取引製品コンテンツ配布に依存する同時的企業活動が可能になる。そのような制御情報および／または制御モデル全体は、制御情報によって決定あるいは許可されるように、コンテンツ、報告、支払いおよび／または関連する制御情報取扱いの経路において異なる参加者に対して異なる方法で与えられ得る。VDEは、異なるパーティ（または例えば、VDEユーザのクラス）が電子情報コンテンツの使用を管理する異なる制御情報を受け取るように、同一のおよび／または異なるコンテンツおよび／または機器使用に関連する活動、および／またはコンテンツおよび／または機器使用モデルにおける異なるパーティへの異なるコンテンツ制御情報の供給をサポートする。例えば、VDE制御されたコンテンツオブジェクトの配布者またはそのようなコンテンツのエンドユーザとしての使用者のカテゴリーに基づいて制御モデルが異なる結果、適用される予算作成が異なり得る。あるいは、例えば、ある一つの配布者は、別の配布者（例えば、光ディスク上に設けられる共通のコンテンツ収集から）とは異なるプロパティのアレイを配布する権利を有し得る。個人および／またはエンドユーザのクラスあるいは他のグループ分けは、「一般的な」コンテンツユーザとは異なるコストを有し得る（例えば、学生、年輩の市民、および／または低所得者のコンテンツユーザであり、同一のあるいは異なる割引を受け得る）。

！　コンテンツおよび／または機器の顧客使用、および／またはプロバイダおよび／またはエンドユーザの税金支払いから、クレジットおよび／または電子通貨のエンドユーザおよび／またはプロバイダからの行政機関への移動によって生じるプロバイダ歳入情報のサポートは、安全な信用される歳入概要情報および／または詳細なユーザ取引リスト（詳細さのレベルは、例えば、取引のタイプまたは

サイズに依存し得る、すなわち、顧客への銀行利子支払いまたは大金（例えば、$10,000を超える）の振替に関する情報は、法律によって自動的に管理機関に報告され得る）を反映する顧客コンテンツ使用情報を含むコンテンツを有するVDEコンテンツコンテナを、そのような受け取られた制御情報が生じさせた結果として「自動的に」生じ得る。課税の対象となる事象および／または通貨および／またはクレジット者通貨振替に関連するそのような概要および／詳細情報は、VDEコンテナ内の管理機関への報告および／または支払い経路に沿って受け渡され得る。そのようなコンテナは、他のVDE関連コンテンツ使用報告情報のためにも用いられ得る。

！　本発明の好ましい実施の形態によると、VDE制御されたコンテンツの制御された多様な配布を受け入れるように、コンテンツ制御情報取扱いの異なる「ブランチ」を介するコンテンツ制御情報の流れをサポートする。それによって、異なるパーティが異なる（おそらくは競合する）制御戦略を用いて、同一の初期電子コンテンツを用いることが可能になる。本例において、コンテンツに対する制御情報を初めに与えたパーティはある制御仮定を行い得、これらの仮定は、より特

定的なおよび／または広範囲の制御仮定に発展する。これらの制御仮定は、例えば、「適切な」コンテンツ制御情報との「ネゴシエーション」において用いるための制御情報交換をコンテンツモデル参加者が提出する際のブランチングシーケンスの間に発展し得る。この結果、新しいあるいは改変されたコンテンツ制御情報が得られ得、および／または適切な別の方法に対するある１つ以上の既に「適切な」コンテンツ使用コントロールメソッドの選択、ならびに関連する制御情報パラメータデータの提出を含み得る。同一の電子プロパティコンテンツ／および機器の異なるコピーに適用される制御情報セットのこの発展形態は、取扱いおよび制御経路全体における異なるブランチを通って「下方に」流れ、これらの異なる経路ブランチを分出するときに異なって改変されるVDE制御情報から生じる。VDEコンテンツ制御情報およびVDE管理コンテンツの両方の流れのための複数の経路ブランチをサポートする本発明の能力によって、相違する競合する企業提携、契約、および例えば、異なる少なくとも一部が競合する商品を表すコンテンツの

異なる収集において組み合わされる同一のコンテンツプロパティを用い得る、発展する企業全体をサポートする電子商取引市場が可能になる。

！　抽出された情報が抽出プロセスを介して継続的に安全に維持されるように、ユーザのVDEインストレーションで安全なサブシステムを用いて、VDEコンテンツコンテナ内に含まれるコンテンツの少なくとも一部をユーザが安全に抽出することを可能にすることによって、新しい安全なオブジェクト（コンテンツコンテナ）を作る。そのような抽出されたコンテンツを含む新しいVDEコンテナが形成される結果、供給源VDEコンテンツコンテナおよび／または適切であれば遠隔VDEインストレーション安全サブシステムコンテンツ制御情報と一致する、あるいはそれによって指定される制御情報が得られる。少なくとも一部がペアレント（供給源）オブジェクトの制御情報から誘導されるセキュリティおよび管理情報などの関連する制御情報は、通常は、抽出されたVDEコンテンツを含む新しいVDEコンテンツコンテナオブジェクトに自動的に挿入される。このプロセスによって、ユーザのVDEインストレーション安全サブシステムで（例えば、１つ以上のパーミッション記録中に暗号化された形態で安全に格納されるこの挿入された制御情報の少なくとも一部を用いて）実行するペアレントオブジェクトの制御枠組みおよび／またはVDEインストレーション制御情報下で一般的に生じる。別の実施の形態において、抽出されたコンテンツに適用される誘導されたコンテンツ制御情報は、遠隔サーバ位置などの安全な抽出を行うVDEインストレーションから遠隔に格納されたコンテンツ制御情報から一部あるいは全体が得られ得るか、あるいはそのコンテンツ情報を用い得る。大半のVDE管理コンテンツについてのコンテンツ制御情報を用いた場合と同様に、本発明の特徴によってコンテンツの制御情報は以下のことが可能になる。

（ａ）「発展」すること。例えば、コンテンツのエクストラクタ（extractor）は、コンテンツの適した制御情報によって可能にされる範囲で、新しい制御情報の追加、および／またはVDEアプリケーションに従う方法などの制御パラメータデータの改変を行い得る。そのような新しい制御情報は、例えば、新しいオブジェクトの少なくとも一部を誰が用い得るか、および／またはどのように抽出され

たコンテンツの少なくとも一部が用いられ得るか（例えば、いつ少なくとも一部が用いられ得るか、あるいは一部のどの部分およびどの量が用いら得るか）を指定し得る。

（ｂ）エクストラクタによって作られるマテリアルおよび／または新しいコンテナへの直接的な配置のために１つ以上の他のVDEコンテナオブジェクトから抽出されたコンテンツ（例えば、イメージ、映像、音声、およびまたはテキスト）などの抽出されたコンテンツの少なくとも一部と付加的なコンテンツを組み合わせることをユーザに可能にすること。

（ｃ）コンテンツをVDEコンテンツコンテナ内に安全な形態で維持しつつ、ユーザがコンテンツの少なくとも一部を安全に編集することを可能にする。

（ｄ）既存のVDEコンテンツコンテナオブジェクトに抽出されたコンテンツを追加し、関連づけられた制御情報を添付すること。これらの場合、ユーザによって付加される情報は安全化、例えば、一部あるいは全体として暗号化され、および適所にあるオブジェクトコンテンツに前に与えられたものとは異なる使用／およびまたは監査制御情報を与えられ得る。

（ｅ）抽出されたコンテンツの１つ以上の部分に対するVDE制御を、その部分の様々な形態の使用後に保護すること。例えば、スクリーンディスプレイ上にコンテンツを「一時的に」可能にしながら、あるいは、ソフトウェアが安全な形態で保持することを可能にしながら、安全に格納された形態にコンテンツを保持するが、そのプログラムの暗号化された実行部分のいすれもを遷移的に復号化する（そのプログラムのすべてあるいは一部が、プログラムを安全化するために暗号化され得る）こと。

一般的に、本発明の抽出特徴によって、安全なVDEケーパビリティを維持しつつ、従って、様々なコンテンツ使用プロセス後にそのコンテンツ情報においてプロバイダの権利を保護しつつ、コンテンツコンテナ供給源から抽出された保護下の電子コンテンツ情報をユーザが集合させ、および／または配信し、および／または使用することが可能になる。

！　VDEによって制御されたコンテンツの部分の集合をサポートする。このよう

な部分は、異なるVDEコンテンツコンテナ制御情報を受ける。様々なこの部分は、集合を行うユーザとは遠隔の１つ以上の異なる位置から独立して異なるコンテンツプロバイダによって提供され得る。本発明の好ましい実施の形態において、このような集合は、例えば、全VDEコンテンツコンテナ内にVDEコンテンツコンテナオブジェクトとしてそのような部分の一部あるいはすべてを個別に埋め込むことおよび／またはそのような部分の一部あるいはすべてをVDEコンテンツコンテナに直接埋め込むことによって、その様々な部分の各々について制御情報（例えば、ロードモジュールなどの実行可能なコード）の少なくとも一部を保護することを含み得る。後者の場合では、このコンテンツコンテナのコンテンツ制御情報は、集合前のこの部分の元の制御情報要件に基づいて様々なそのような部分に異なる制御セットを与え得る。そのような埋込みVDEコンテンツコンテナの各々は、１つ以上のパーミッション記録の形態でそれ自体の制御情報を有し得る。あるいは、電子コンテンツの様々な集合された部分と関連づけられる制御情報間のネゴシエーションによって、集合されたコンテンツ部分の一部あるいはすべてを管理する制御情報セットが生成され得る。ネゴシエーションによって生じるVDEコンテンツ制御情報は均一であっても（同一ロードモジュールおよび／またはコンポーネ

ントアセンブリを有するなど）、および／または異なる計量、予算作成、課金および／または支払いモデルなどのVDE制御コンテンツの集合を構成する２つ以上の部分に異なるそのようなコンテンツ制御情報を与えてもよい。例えば、コンテンツ使用支払いは、情報交換所を介してあるいは直接に、異なる部分について異なるコンテンツプロバイダに行われ得る。

！　電子コンテンツおよび／または電子機器の使用に関連する情報のフレキシブルな計量あるいは他の収集を可能にする。本発明の特徴は、計量制御メカニズムが以下の同時の広いアレイを含むことを可能にする。（ａ）電子情報コンテンツ使用に関連する異なるパラメータ、（ｂ）異なるインクリメントユニット（バイト、文書、プロパティ、パラグラフ、イメージなど）および／またはそのような電子コンテンツの他の編成、および／または（ｃ）クライアント組織、部署、プ

ロジェクト、ネットワーク、および／または個人ユーザなどの、ユーザの異なるカテゴリーおよび／またはVDEインストレーションタイプ。本発明の特徴は、コンテンツセキュリティ、使用分析（例えば、市場観測）、および／または使用および／またはVDE管理コンテンツへの露出に基づく補償のために用いられ得る。そのような計量は、コンテンツ使用料、ライセンス取得、購入、および／または広告に対する支払いを保証するためのフレキシブルな基礎である。本発明の特徴によって、電子通貨およびクレジットの使用に関連する情報を反映する監査追跡を安全に維持する能力を含む、フレキシブルなそのような通貨およびクレジットのメカニズムをサポートする支払い手段が提供される。VDEは、クラインアント組織制御情報の複数の異なる階層をサポートし、ここで、組織クラインアント管理者は、部署、ユーザおよび／またはプロジェクトの使用権を指定する制御情報を配布する。同様に、部署（部門）ネットワークマネージャは、部署ネットワーク、プロジェクトおよび／またはユーザなどのための配布者（予算作成、アクセス権など）として機能し得る。

！　安価な消費者（例えば、テレビセットトップ機器）および専門機械（および手のひらサイズのPDA）からサーバ、メインフレーム、通信スイッチなどにわたる電子機器上で使用するための規模可変（scalable）で統合可能な標準化された制御手段を提供する。本発明の規模可変な取引管理／監査技術によって、電子商

取引および／またはデータセキュリティ環境において機能する装置間でのより効率的で信頼性のある相互動作性が得られる。標準化された物理的コンテナが、世界中への物理的商品の出荷に必要不可欠になり、これらの物理的コンテナが積み下ろし機器に普遍的に「適合」し、トラックおよび列車の空間を有効に用い、効率的にオブジェクトの公知のアレイ（例えば、箱）を収容することが可能になると、VDE電子コンテンツコンテナは、本発明によって提供されるように、電子情報コンテンツ（商業的に発行されたプロパティ、電子通貨およびクレジットおよびコンテンツ監査情報）および関連づけられたコンテンツ制御情報を効率的に世界中に移動させることが可能になる。相互動作性は、効率的な電子商取引の基礎である。VDE基礎、VDEロードモジュール、およびVDEコンテナの設計は、VDEノー

ド動作環境を、非常に広範な電子機器と互換性を有させる重要な特徴である。例えば、ロードモジュールに基づくコントロールメソッドを、非常に小さい読み出し／書込みメモリを有する環境などの非常に「小型の」および安価な安全なサブシステム環境において実行し、同時により高価な電子機器において実行し得る能力は、多くの機械にわたって一貫性をサポートする。その制御構造およびコンテナアーキテクチャを含むこの一貫したVDE動作環境によって、幅広い装置タイプおよびホスト動作環境にわたって標準化されたVDEコンテンツコンテナの使用を可能にする。VDEケーパビリティは、電子機器およびホスト動作システムの基本的なケーパビリティに対する拡張、付加および／または改変として継き目なく統合され得るので、VDEコンテナ、コンテンツ制御情報およびVDE基礎は、多くの装置タイプと共に作動することが可能であり、これらの装置タイプは一貫しておよび効率的にVDE制御情報を翻訳および実施することができる。この統合化を介してユーザは、VDEの多くのケーパビリティとのトランスペアレントな相互作用からの利益を得ることができる。ホスト電子機器上で動作するソフトウェアとのVDE統合化は、そのような統合がなければ利用不可能であるかあるいは安全性が低い様々なケーパビリティをサポートする。１つ以上の装置アプリケーションおよび／または装置動作環境との統合化を介して、本発明の多くのケーパビリティが与えられた電子機器、オペレーティングシステムあるいは機器アプリケーションの本質的なケーパビリティとして提示され得る。例えば、本発明の特徴は、

（ａ）ホストオペレーティングシステムが安全な取引処理および電子情報格納を可能にするなどのVDEケーパビリティを所有するように、ホストオペレーティングシステムを一部拡張および／または改変するためのVDEシステムソフトウェア、（ｂ）VDE動作と関連づけられるツールを一部表す１つ以上のアプリケーションプログラム、および／または（ｃ）アプリケーションプログラムに組み込まれるコードであって、そのようなコードはVDEケーパビリティを統合するためにリファレンスをVDEシステムソフトウェアに組み込み、そのようなアプリケーションをVDE認識にする（例えば、ワードプロセッサ、データベース検索アプリケーション、スプレッドシート、マルチメディアプレゼンテーションオーサリングツ

ール、映画編集ソフトウェア、MIDIアプリケーションなどの音楽編集ソフトウェア、ＣＡＤ／ＣＡＭ環境およびＮＣＭソフトウェアなどに関連づけれたものなどのロボット制御システム、電子メールシステム、電子会議ソフトウェア、および他のデータのオーサリング、生成、取扱い、および／または上記の組み合わせを含む使用アプリケーション）。これらの一つ以上の特徴（ファームウェアあるいはハードウェアにおいても実施され得る）は、マイクロコントローラ、マイクロプロセッサ、他のCPUまたは他のディジタル処理論理などのVDEノード安全なハードウェア処理ケーパビリティと共に用いられ得る。

！　通常はネットワークベースの取引処理再調停（reconciliation）およびしきい値チェック活動を介して、VDE構成のセキュリティのある侵害が生じたかを評価する監査再調停および使用パターン評価プロセスを用いる。これらのプロセスは、例えば、与えられたVDEインストレーションによって電子プロパティについて例えば、購入および／または要求を評価することによってVDE制御されたコンテンツエンドユーザVDE位置に遠隔に行われる。そのような調停活動のためのアプリケーションは、遠隔に配達されたVDE制御されたコンテンツの量がそのようなコンテンツの使用のために用いられる金融クレジットおよび／または電子通貨の量に対応するかの評価を含む。信頼できる組織は、与えられたVDEインストレーションおよび／またはユーザに与えられたコンテンツのコストに関してコンテンツプロバイダから情報を獲得し、このコンテンツのコストをそのインストレーションおよび／またはユーザのクレジットおよび／または電子通貨支出と比較する。支出量に対する配送されたコンテンツ量における非一貫性は、状況に応じて、遠隔VDEインストレーションが少なくともある程度侵犯されたか（例えば、１つ以上の鍵を暴露することによって安全なサブシステムおよび／またはVDE制御されたコンテンツの少なくとも一部の暗号を解説するなどの、ある重要なシステムセキュリティ機能）を証明および／または示し得る。コンテンツ使用の不規則なパターン（例えば、非常に高い要求）、または１つ以上のVDEインストレーションおよび／またはユーザ（例えば、疑わしい使用の集合パターンを有する、関連するユーザのグループを含む）は、そのような１つ以上のインストレーション

における および／またはそのような１人以上のユーザによるセキュリティが、特に、１つ以上のVDEユーザおよび／またはインストレーションに与えられる電子クレジットおよび／または通貨の判断と組み合わせられて用いられたときに、そのようなユーザおよび／またはインストレーションによって行われる支出と比較すると、それらのクレジットおよび／または通貨供給者の一部あるいは全体によって侵犯されたかの判定にも有用であり得る。

！　システムの統合性を「壊す」ために必要な時間を物質的に増加させるセキュリティ技術をサポートする。これは、本発明のセキュリティ特性のいくつかの面を含むことから生じる損害を最小化する技術の集まりを用いることを含む。

！　本発明の信頼できる／安全な、世界規模の分散型の取引制御および管理システムのコンポーネントを含む、オーサリング、管理上、報告、支払いおよび課金ツールユーザアプロケーションの集合を提供すること。これらのコンポーネントは、VDEに関連する、オブジェクト生成（制御情報をコンテンツ上に配置することを含む）、安全なオブジェクト配布および管理（配布制御情報、金融関連および他の使用分析を含む）、クライアント内部VDE活動管理および制御、セキュリティ管理、ユーザインタフェース、支払い支出、および情報交換所関連機能をサポートする。これらのコンポーネントは、非常に安全で、均一かつ一貫し標準化された、処理、報告および／または支払いの電子商取引および／またはデータセキュリティ経路、コンテンツ制御および管理、および人的ファクタ（例えば、ユーザインタフェース）をサポートするように設計されている。

！　例えば、使用情報管理を含むVDE構成の組織の使"用における補助を行うため

に大型組織においてクライアント管理者によって行われる活動などの、金融およびユーザ情報交換所活動、およびクライアント管理者によって提出される情報を制御するために一連の制御情報に供されるクライアント人員のあるグループおよび／または個人のためのVDE下で利用可能な予算および使用権の特徴を指定するなどの、雇用人個人あるいはグループによるVDE活動の制御を含む、複数の情報交換所の動作をサポートする。情報交換所では、１つ以上のVDEインストレーションが、信頼できる分散データベース環境（同時データベース処理手段を含み得

る）と共に動作し得る。金融情報交換所は、通常、その位置で安全に配送されたコンテンツ使用情報およびユーザ要求（別のクレジット、電子通貨および／またはより高いクレジット制限など）を受け取る。使用情報およびユーザ要求の報告は、電子通貨、課金、支払いおよびクレジット関連活動、および／またはユーザプロファイル分析および／またはより広い市場観測分析をサポートするため、および（統合された）リスト生成あるいは、少なくとも一部が上記の使用情報から得られる他の情報のマーケティングのために用いられ得る。この情報は、VDEインストレーション安全サブシステムに安全な認証された暗号化通信を介して、コンテンツプロバイダあるいは他のパーティに与えられ得る。情報交換所処理手段は、通常は、情報交換手段と他のVDE経路参加者との間の安全な通信のために用いられ得る高速遠隔通信切替手段を含み得る特殊化されたI/O手段に接続される。

！　電子通貨およびクレジット使用制御、格納およびVDEインストレーションにおけるおよびVDEインストレーション間の通信を安全にサポートする。VDEはさらに、支払い経路を介する支払いトークン（電子通貨またはクレジットの形態でのような）あるいは他の支払い情報を含む、電子通貨および／またはクレジット情報の自動化された通過をサポートし、この経路は、コンテンツ使用情報報告経路と同じであっても同じでなくてもよい。このような支払いは、VDE制御電子コンテンツおよび／または機器の使用から生じる所有された量に基づく電子クレジットまたは通貨アカウントからのクレジットまたは電子通貨の「引き出し」を規定する制御情報に応答してVDEインストレーションによって自動的に生成されたVDEコンテナ中に配置され得る。そして、支払いクレジットまたは通貨は、VDEコンテナの遠隔通信を介して、情報交換所、元のプロパティコンテンツまたは機器のためのプロバイダ、またはそのようなプロバイダ（情報交換所以外）のためのエージェントなどの適切なパーティと自動的に通信し得る。支払い情報は、計量情報などの関連するコンテンツ使用情報を有するあるいは有さない上記のVDEコンテンツコンテナ中にパッケージされ得る。本発明の一つの局面によって、通過使用に関するある情報を、ある、一部のあるいはすべてのVDEパーティ（「条件付

きで」完全に匿名の通貨）に利用不可能であるものとして指定することを可能にし、および／または、通貨および／またはクレジット使用関連情報（および／または電子情報使用データ）などのあるコンテンツ情報を、裁判所の命令（「条件付きで」匿名の情報に安全にアクセスするために必要であり得る裁判所により制御されるVDEインストレーションの使用を介する承認をそれ自体が必要とし得る）などのある厳しい条件下のみで利用可能にするように規制し得る。通貨およびクレジット情報は、本発明の好ましい実施の形態では、管理上のコンテンツとして扱われる。

！　本発明により保護下のコンテンツが（表示され、印刷され、通信され、抽出され、および／または保存された）VDEオブジェクトから明確な形態で放出されると、ユーザの身分を表す情報および／またはコンテンツを明確な形態に変形させる責任を負うVDEインストレーションが放出されたコンテンツの中に埋めこまれるように、コンテンツへの埋込みのための指紋刻印（透かし模様としても知られる）をサポートする。指紋刻印は、VDEコンテナから明確な形態で情報を抽出した人、あるいはVDEオブジェクトのコピーあるいはそのコンテンツの一部を作成した人を識別する能力の提供に有用である。ユーザの識別および／または他の識別情報は不明瞭に、あるいは概して隠匿されてVDEコンテナコンテンツおよび／または制御情報に埋め込まれ得るので、潜在的な著作権侵害者が非承認抽出あるいはコピーを行うことを防止し得る。指紋は暗号化されたコンテンツに埋め込まれ、後に、指紋情報を有する暗号化されたコンテンツが復号化されると安全なVDEインストレーションサブシステム中の非暗号化コンテンツ中に配置され得るが、指紋は、通常、非暗号化電子コンテンツあるいは制御情報に埋め込まれる。VDEコンテナのコンテンツなどの電子情報は、受け取りを行うパーティに向けたネットワーク（インターネットなど）位置を離れるので、指紋刻印がされ得る。

そのような格納場所情報は、通信の前には非暗号化形態で維持され、格納場所を離れるときに暗号化され得る。指紋刻印は、好ましくは、コンテンツが格納場所を離れるときに、暗号化ステップの前に生じ得る。暗号化された格納場所コンテンツは、例えば、安全なVDEサブシステム中で復号化され、指紋情報が挿入され

、次いで、コンテンツは伝送のために再暗号化され得る。意図された受取人ユーザの識別情報および／またはVDEインストレーションを、コンテンツが、例えば、インターネット格納場所から離れるときにコンテンツに埋め込むことによって、VDEインストレーションあるいは配送されたコンテンツのセキュリティの侵犯を管理したいずれものパーティを識別あるいはその識別の補助をする重要な情報を提供する。承認された明確な形態のコピーの非承認コピーの作成を含む、VDE制御コンテンツの承認された明確な形態のコピーをパーティが作る場合は、指紋情報は、個人および／またはその個人のVDEインストレーションを再び指し示す。そのような隠された情報は、潜在的なコンテンツ「侵害」の大半の部分に他のパーティの電子情報を盗むことを行わせなくすべきである、行動を妨げる強力な行為として働く。受け取りを行うパーティおよび／またはVDEインストレーションを認識する指紋情報は、VDEコンテンツオブジェクトの復号化、複製あるいは受取者への通信の前あるいは間に、VDEオブジェクトに埋め込まれ得る。消費者あるいは他のユーザへの移動のために電子情報を暗号化する前に電子情報の指紋刻印は、非暗号化形態で配布されたあるいは利用可能にされ得るあるコンテンツを受け取った人を識別するために非常に有用であり得る情報を提供する。この情報は、VDEインストレーションのセキュリティを「破り」得、非合法的にある電子情報を他人に利用可能にした人の追跡に有用である、指紋刻印によって、上記のコンテンツ情報の放出（例えば、抽出）時間および／または日などの、付加的な利用可能な情報を提供し得る。指紋を挿入するための位置は、VDEインストレーションおよび／またはコンテンツコンテナ制御情報によって指定され得る。この情報は、１つ以上のある情報フィールドあるいは情報タイプなどの、プロパティ内のある領域および／または正確な位置が、指紋刻印のために用いられるべきであることを指定し得る。指紋情報は、色周波数および／またはある画像画素の輝度を通常は検出不可能に改変することによって、周波数に関してある音声信号を

わずかに改変することによって、フォント文字形成を改変することなどによってプロパティに組み込まれ得る。指紋情報自体は、不正改変された指紋を有効であ

ると解釈することを特に困難にするように暗号化されるべきである。同一プロパティの異なるコピーのための指紋位置の変化、「偽の」指紋情報、および特定のプロパティあるいは他のコンテンツ内の指紋情報の複数のコピーであって、情報配布パターン、周波数および／または輝度加工および暗号化関連技術などの異なる指紋刻印技術を用いるコピーは、非承認個人が、指紋位置を識別し、指紋情報を消去および／または改変することをさらに困難にするための本発明の特徴である。

！　予算作成、承認、クレジットまたは通貨、およびコンテンツを含む要求、データ、および／またはメソッドを運搬し得るスマートオブジェクトエージェントを提供する。例えば、スマートオブジェクトは、遠隔情報リソース位置へおよび／またはから移動し、電子情報コンテンツについての要求を満たし得る。スマートオブジェクトは、例えば、遠隔位置に伝達され、それによってユーザを代表して指定されたデータベース検索を行うか、あるいはユーザが望む情報についての情報の１つ以上の格納場所を「知的に」遠隔に検索する。例えば、１つ以上のデータベース検索を行うことによって、１つ以上の遠隔位置で所望の情報を識別した後は、スマートオブジェクトは、検索された情報を含む安全な「リターンオブジェクト」の形態で通信を介してユーザに戻り得る。ユーザは、情報の遠隔検索、ユーザのVDEインストレーションへの情報の帰還、および／またはそのような情報の使用に対して課金され得る。後者の場合では、ユーザは、ユーザが実際に使用するリターンオブジェクトにおける情報についてのみ課金され得る。スマートオブジェクトは、１つ以上のサービスおよび／またはリソースの使用を要求する手段を有し得る。サービスは、他のサービスおよび／または情報リソースなどのリソースの配置、言語またはフォーマット変換、処理、クレジット（あるいは付加的なクレジット）承認などを含む。リソースは、参照データベース、ネットワーク、高電力あるいは特殊化演算リソース（スマートオブジェクトは、他のコンピュータに情報を運搬し、それによって情報を効率的に処理し、次いで情報を送り出しVDEインストレーションに戻し得る）、遠隔オブジェクト格納場所などを

含む。スマートオブジェクトは、実際使用された情報および／またはリソースに基づいてユーザに課金を行うための安全な手段を提供すると同時に、遠隔リソース（例えば、集中データベース、スーパーコンピュータなど）を効率的に使用させ得る。

！　VDE電子契約エレメントの近代言語印刷契約エレメント（英語の契約など）への「翻訳」および電子権利保護／取引管理近代言語契約エレメントの電子VDE契約エレメントへの翻訳の両方をサポートする。この特徴は、VDEロードモジュールおよび／またはメソッドおよび／またはコンポーネントアセンブリに対応するテキスト言語のライブラリの維持を必要とする。VDEメソッドがVDE契約について提案および／または用いられるので、テキスト用語および条件のリストは、好ましい実施の形態において、格納され、上記のメソッドおよび／またはアセンブリに対応する句、文、および／または段落を提供するVDEユーザアプリケーションによって生成され得る。この特徴は、好ましくは、法律的あるいは記述的文書の一部あるいはすべてを構成するように選択されたメソッドおよび／またはアセンブリに対応するライブラリエレメント間の適切な順序および関係を、分析および自動的に決定するおよび／または１人以上のユーザの決定を補助するための人工知能ケーパビリティを用いる。１人以上のユーザおよび／または好ましくは法定代理人（文書が法的な拘束力のある契約である場合）、完成時に作成された文書資料を再検討し、そのような付加的なテキスト情報および／または契約の非電子取引エレメントを記載し、必要であり得る他のいずれもの改善を行うために必要であるような編集を用いる。これらの特徴はさらに、一人以上のユーザが選択肢から選択を行い、質問に答えを与え、そのようなプロセスからVDE電子契約を生じさせることを可能にする近代言語ツールの使用をサポートする。このプロセスはインタラクティブであり、VDE契約公式化プロセスは、応答から学習し、また、適切でありその応答に少なくとも一部が基づく場合、所望のVDE電子契約を「発展」させるさらなる選択肢および／または質問を提供する、人工知能エキスパートシステム技術を用い得る。

！　単一のVDEインストレーションにおける複数のVDE安全サブシステムの使用を

サポートする。様々なセキュリティおよび／または性能の利点は、分散型のVDE設計を単一のVDEインストレーション内で用いることによって実現され得る。例えば、ハードウェアベースのVDE安全サブシステムを電子機器VDEディスプレイ装置内に設計すること、および表示点にできるだけ近づくようにディスプレイ装置とサブシステムとの統合化を設計することによって、ビデオシステム外部から内部へ移動するに従って復号化されたビデオ情報を「盗む」ことを物質的により困難にし、それによって、ビデオ材料に対するセキュリティが増す。理想的には、例えば、VDE安全ハードウェアモジュールは、ビデオモニタあるいは他の表示装置のパッケージ内にあるように、実際の表示モニタと同じ物理的パッケージ内にあり、そのような装置は、商業的に実用可能な範囲で合理的に不正改変不可能なものとして設計される。別の実施例において、VDEハードウェアモジュールのI/O周辺装置への埋め込みは、システムスループット全体の見地からある利点を有し得る。複数のVDE例が同一のVDEインストレーション内で用いられる場合、VDE例が同一の大容量記憶装置上におよび同一のVDE管理データベース内にある制御情報およびコンテンツおよび／または機器使用情報を格納するなどのように、これらの例は理想的には実用的な程度にまでリソースを共有する。

！　予算の枯渇および鍵の経時エージング(time ageing)の使用によって報告および支払いコンプライアンスを要求する。例えば、VDE商業的構成および関連づけられるコンテンツ制御情報は、コンテンツプロバイダのコンテンツおよびそのコンテンツのエンドユーザ使用に対する支払いのための情報交換所クレジットの使用を伴い得る。この構成に関する制御情報は、（そのコンテンツの）ユーザのVDEインストレーションおよびその金融情報交換所のVDEインストレーションに配送され得る。この制御情報は、ある形態のコンテンツ使用ベース情報、および電子クレジット（そのようなクレジットは、受け取り後にプロバイダによって「所有」され、電子通貨の利用可能性および妥当性の代わりに用いられ得る）および／または電子通貨の形態のコンテンツ使用支払いの両方を、上記の情報交換所が準備し、コンテンツプロバイダに遠隔通信することを必要とする。情報および支払いのこの配達は、安全に、およびいくつかの実施の形態においては自動的に、上記の制御情報によって指定される方法で提供するために、信頼できるVDEイン

ストレーション安全サブシステムを用い得る。本発明の特徴によって、そのような使用情報および支払いコンテンツの情報交換所の報告が見られ得るという要件を保証し得る。例えば、VDE電子契約への１人の参加者がそのような情報報告および／または支払い義務を見ることができない場合、別の参加者は、法律侵犯パーティのそのような契約に関連するVDE活動への参加を停止し得る。例えば、要求される使用情報および支払いがコンテンツ制御情報によって指定されるように報告されない場合、「傷ついた（injured）」パーティは、そのVDEインストレーション安全サブシステムから安全に通信できないことによって、一連の１つ以上の重大なプロセスに必要な機密情報の１つ以上の部分を提供し得ない。例えば、情報交換所からコンテンツプロバイダに情報および／または支払いを報告できない（ならびにいずれものセキュリティ欠陥または他の妨害的な不正行為がある）と、コンテンツプロバイダは情報交換所に鍵および／または予算リフレッシュ情報を与え得ない。この情報は、プロバイダのコンテンツの使用についての情報交換所のクレジットの使用を承認するために必要になり得、この情報交換所は、情報交換所とエンドユーザとの間のコンテンツ使用報告通信間にエンドユーザと通信する。別の実施例として、支払いおよび／またはコンテンツプロバイダへの使用情報の報告を行えなかった配布者は、ユーザにコンテンツプロバイダのコンテンツを配布するためにパーミッション記録を作成するための予算および／またはプロバイダのコンテンツのユーザの使用の一つ以上の他の側面を制限するセキュリティ予算は、一旦消耗されるまたは一次中止になると（例えば、所定の日付に）、コンテンツプロバイダによってリフレッシュされないことを見出し得る。これらのおよび他の場合においては、違反したパーティは「エージアウト（aged out）」した経時エージング鍵をリフレッシュしないことを決定し得る。そのような経時エージング鍵の使用は、予算および経時エイジング承認をリフレッシュし得ないので、同様の影響を有する。

！　安全なクレジット、銀行、および／または金銭カードとして用いられ得るカードを含む、携帯電子機器の形態で本発明のスマートカード実施をサポートする。本発明の特徴は、小売りおよび他の制度で取引カードとしての携帯VDEの使用である。ここで、そのようなカードは、VDE安全サブシステムおよび／またはVDE

安

全および／または、「信頼できる」金融情報交換所（例えば、VISA、Mastercard）などの安全な互換性のあるサブシステムを有する秩序端末と「接続（dock）」し得る。クレジットおよび／または電子通貨が商人および／または情報交換所に転送され、取引情報がカードに再び流れる状態で、VDEカードおよび端末（および／またはオンライン接続）は取引に関連する情報を安全に交換し得る。このようなカードは、すべての種類の取引活動のために用いられ得る。パーソナルコンピュータなどの電子機器上のPCMCIAコネクタなどのドッキングステーションは、家で消費者のVDEカードを受け取り得る。そのようなステーション／カードの組み合わせは、そのような電子機器において永続的にインストールされるVDEインストレーションと同じ方法で、オンライン取引のために用いられ得る。カードは「電子財布」として用いられ、電子通貨および情報交換所によって供給されるクレジットを含む。カードは、ホームバンキング活動を含む（すべてではないにせよ）多くの商業、銀行業務およびオンライン金融取引に関する消費者の金融活動のための収束点として働き得る。消費者は、オンライン接続を介して、給料支払い小切手および／または投資収入および／またはそのような受け取りに関する「信頼のおける」VDEコンテンツコンテナに安全化された詳細情報を受け取り得る。ユーザは、VDE構成を用いて他のパーティにディジタル通貨を送り得、これはそのような通貨を与えることを含む。VDEカードは、金融的に関連する情報が合併され、かつ非常に容易に検索および／または分析されるように、非常に安全かつデータベースによって組織化された方法で取引の詳細を保持し得る。効率的な暗号化、認証、ディジタル署名、および安全なデータベース構造を含むVDEセキュリティがあるために、VDEカード構造内に含まれる記録は、管理のための有効な取引記録および／または一体の記録保護要件として許容され得る。本発明のいくつかの実施の形態において、VDEカードは、ドッキングステーションおよび／または電子機器記憶手段を使用および／または上記の機器に遠隔なおよび／またはネットワークを介して利用可能な他のVDE構成手段を共有して、例えば、日付をつけたおよび／または保管されたバックアップ情報を格納することによって、

VDEカードの情報格納容量を増加させる。個人の金融活動の一部あるいはすべてに関連する税金は、安全に格納され上記のVDEカードに利用可能な「信頼の

おける」情報に基づいて、自動的に演算され得る。上記の情報は、上記のカード、上記のドッキングステーション、上記の関連づけられた電子機器、および／またはそれらに動作可能に取り付けられた、および／または遠隔サーバサイトなどに遠隔に取り付けられた他の装置に格納され得る。カードのデータ、例えば、取引履歴は、個人のパーソナルコンピュータあるいは他の電子機器にバックアップされ得、そのような機器は、それ自体の統合化されたVDEインストレーションを有し得る。現在の取引、最近の取引（リダンダンシーのため）、あるいはすべてのまたは他の選択されたカードデータは、ユーザ／商人取引などの金融取引および／または情報通信のための各々のまたは周期的なドッキングの間に、金融情報交換所のVDE互換格納場所などの遠隔バップアップ格納場所にバックアップされ得る。取引情報を遠隔情報交換所および／または銀行に輸送することによって、別のパーティのVDEインストレーション（例えば、金融あるいは汎用電子ネットワーク上のVDEインストレーション）との接続の間に少なくとも現在の取引をバックアップすることは、カード不良または紛失の場合にVDEカード内部情報の完全な再構築を可能にするために十分なバックアップが行われることを保証し得る。

！　仕様プロトコルが他のVDE構成および／またはインストレーションから許容不可能に偏差しているVDE構成および／またはインストレーションが、セキュリティ（VDE安全化情報の統合性および／または安全性）、プロセス制御、および／またはソフトウェア互換性の問題を導入し得るように相互動作することを防止するように、様々なVDEインストレーション間の承認された相互動作性を保証する証明プロセスをサポートする。証明は、VDEインストレーションの識別および／またはそれらのコンポーネント、ならびにVDEユーザの有効性を示す。証明データは、VDEサイトに関連する撤退、あるいは他の変更の決定に寄与する情報となり得る。

！　イベントベースの（イベントによってトリガされる）メソッド制御メカニズムの使用による、基本的取引制御プロセスの分離をサポートする。これらのイベ

ントメソッドは、１つ以上の他のVDEメソッド（安全なVDEサブシステムに有効である）をトリガし、VDEによって管理された取引に関連する処理を実行するために用いられる。これらのトリガされたメソッドは、独立して（別々に）および安全に処理可能なコンポーネント課金管理メソッド、予算作成管理メソッド、計量管理メソッド、および関連する監査管理プロセスを含む。本発明がこの特徴、すなわち計量、監査、課金および予算作成メソッドの独立したトリガ、を有する結果、本発明は、複数の金融通貨（例えば、ドル、マルク、円）およびコンテンツに関連する予算、および／または課金インクリメントならびに非常にフレキシブルなコンテンツ配布モデルを効率的に並行してサポートすることができる。

！（１）コンテンツイベントトリガ、（２）監査、（３）予算作成（使用権がないことあるいは使用権に制限がないことの指定を含む）、（４）課金、および（５）ユーザアイデンティティ（VDEインストレーション、クライアントの名前、部署、ネットワーク、および／またはユーザなど）に関連する制御構造の完全なモジュラー分離をサポートする。これらのVDE制御構造が独立していることによって、これらの構成の２つ以上の間の複数の関係を可能にするフレキシブルなシステム、例えば、金融予算を異なるイベントトリガ構造（その論理的部分に基づくコンテンツの制御を可能にするために適切な場所に配置される）と関連づける能力を提供する。これらの基本VDEケーパビリティ間にそのような分離がなければ、別々の計量、課金、予算作成および識別、および／または、例えば、コンテンツ使用と関連づけられる料金支払い、ホームバンキングを行うこと、広告サービスを管理することなどの、計量、課金、予算作成およびユーザ識別のための同一の、異なる（重畳を含む）、または全く異なる部分を含む課金活動を効率的に維持することはより困難になる。これらの基本ケーパビリティのVDEモジュラー分離は、１つまたは異なるコンテンツ部分（および／または部分ユニット）の間の複数の「任意の」関係のプログラミング、予算作成、監査および／または課金制御情報をサポートする。例えば、VDE下では、一月に200ドルまたは300ドイツマルクの予算制限があるデータベースの復号化のために適用され、その復号化されたデータベースが記録される度に（ユーザが選択した通貨に依存して）２U.S.

ドルまたは３ドイツマルクが請求され得る。そのような使用は計量され、ユーザプロファイル目的のための付加的な監査が準備され、各ファイルされ表示されたアイデンティティを記録し得る。さらに、さらなる計量が、復号化されたデータベースバイト数に関して行われ得る。また、関連するセキュリティ予算によって、毎年そのデータベースの全バイトの５％を越える復号化を防止し得る。また、ユーザは、VDE下で（上位の制御情報によって許可される場合）、異なる個人およびクライアント組織部署によってデータベースフィールドの使用を反映する監査情報を収集し得る。また、ユーザは、アクセスの異なる権利およびデータベースを制限する異なる予算が、これらのクライアント個人およびグループに適用され得ることを保証する。コンテンツプロバイダおよびユーザによるユーザ識別、計量、予算作成、および課金制御情報のそのような異なるセットの実際の使用は、一部は、そのような独立制御ケーパビリティの使用の結果として行われる。その結果、VDEは、同一の電子プロパティに適用される複数の制御モデル、異なるまたは完全に異なるコンテンツモデル（例えば、ホームバンキングに対する電子ショッピング）に適用される同一のおよび／または複数の制御モデルの形成において、高い構成性をサポートし得る。

メソッド、他の制御情報およびVDEオブジェクト

VDE管理プロパティ（データベース、文書、個人の商業的製品）の使用をひとまとめに制御するVDE制御情報（例えば、メソッド）は、コンテンツ自体と共に（例えば、コンテンツコンテナに入れられて）輸送されるか、および／またはそのような制御情報の一つ以上の部分が配布者および／または別々に配送可能な「管理上のオブジェクト」中の他のユーザに輸送される。プロパティのためのメソッドのサブセットは各プロパティと共に一部が配送され、メソッドの１つ以上の他のサブセットがユーザに別々に配送されるか、または使用のために利用可能に（遠隔通信手段によって遠隔に利用可能になるなどのように）され得る。要求されるメソッド（プロパティおよび／または機器使用に必要になるように列挙されたメソッド）は、VDE制御コンテンツ（VDEコンテンツコンテナ内で配布される知

的プロパティなど）が使用される場合に指定されるように利用可能であるべきである。コンテンツを制御するメソッドは、そのようなオブジェクトのクラスあるいは他のグループわけのような、複数のVDEコンテナオブジェクトにあてはまり得る。また、そのようなパーティについてのあるユーザ、あるいはユーザのクラスおよび／またはVDEインストレーションおよび／またはインストレーション

のクラスによって、メソッドが１つ以上の特定的なオブジェクトあるいはオブジェクトのクラスを使用することが要求され得る。

本発明によって提供されるVDEの特徴は、VDEインストレーションおよび／またはユーザがあるコンテンツの一部および／またはすべてを使用し得るようにするために必要になるように、ある一つ以上のメソッドが指定され得ることである。例えば、エンドユーザに復号化されたコンテンツを電子的にセーブすることを禁止するメソッドをあるタイプのコンテンツの配布者が必要とすることを、「上位の」参加者（例えば、コンテンツクリエータ）によって許可され、VDE取引のためのクレジットのプロバイダは、電子購入の時間を記録する監査メソッドを必要とし、および／またはユーザは、使用行為の詳細に関する秘密の秘密情報を運ばないように情報交換所に報告するための使用情報（例えば、課金情報）を要約するメソッドを必要とし得る。

本発明によって提供されるVDEのさらなる特徴は、コンテンツのクリエータ、配布者およびユーザが、コンテナコンテンツ使用および配布機能を制御するために予め定義されたメソッド（利用可能である場合）のセットから選択することができ、および／またはコンテンツのクリエータ、配布者およびユーザが、少なくとも一部の使用機能を制御するためのカスタマイズされた新しいメソッド（そのような「新しい」メソッドは、VDEインストレーションおよび／またはVDEアプリケーションのグループへの信頼性および相互動作性について証明される必要があり得る）を提供する権利があり得る。その結果、VDEは、各プロパティまたはオブジェクト（または、所望のようにおよび／または適用可能なようにオブジェクトまたはプロパティの一つ以上の部分）の配布および他の使用がどのように制御されるかに関して非常に高い程度の構成性を提供する。コンテンツ制御情報のVD

E経路における各VDE参加者は、そのような制御情報が既に所定位置にある上位の制御情報と以下に関して対立しない限り、VDEコンテナ内のコンテンツの一部またはすべてのためのメソッドを設定し得る。

（１）VDE管理コンテンツの一部またはすべて、

（２）ある一つ以上のVDEユーザおよび／またはユーザのグループ、

（３）ある一つ以上のVDEノードおよび／またはノードのグループ、および／

または

（４）ある１つ以上のVDEアプリケーションおよび／または構成。

例えば、あるコンテンツについてのコンテンツクリエータのVDE制御情報は、他の提出されたVDE参加者制御情報に対して優位になる。また、例えば、上位の制御情報が許可する場合、コンテンツ配布者の制御情報自体がクライアント管理者の制御情報に対して優位になり得、エンドユーザの制御情報に対して優位になり得る。そのような電子コンテンツ制御情報を設定する配布参加者の能力の経路は、ある制御情報（例えば、価格設定および／または販売日などの方法を介在するデータ）に限定されるか、あるいは、１つ以上の参加者の提案制御情報が、プロパティの取扱いのチェーンにおいて参加者によって前もって提出された、あるいは上記の参加者のVDE安全サブシステムにおいて管理される上位の制御情報によって設定される制御情報と対立する程度のみに制限され得る。

VDE制御情報は、一部あるいは全てが、（ａ）VDEコンテンツ制御情報経路参加者によって所定位置に直接置かれた制御情報を表し、および／または（ｂ）電子コンテンツ（または電子機器）パーミッション記録情報（例えば、金融情報交換所あるいは行政機関を代表する参加者によって挿入された制御情報）を直接取り扱わないパーティを代表するそのような参加者によって所定位置に置かれた制御情報を含む。そのような制御情報メソッド（および／またはロードモジュールおよび／または介在するデータおよび／またはコンポーネントアセンブリ）は、提出された制御情報の１つ以上の部分の使用が既存の制御情報に組み込まれるか、および／または既存の制御情報の代わりになるか（および／またはインプレース制御情報との相互作用に基づいて別の制御情報の間で選択を行うか）およびどの

ような制御情報がどのように用いられ得るかを判断する電子自動化された、または半自動化され人間によって補助される制御情報（制御セット）ネゴシエーションプロセスによって、インプレースに配置され得る。

制御情報は、電子コンテンツ（および／または機器）および／またはそのようなコンテンツ（および／または機器）のための制御情報の取扱いに直接参加しないパーティによって提供され得る。そのような制御情報は、そのような直接に参加しない1つ以上のパーティのVDEインストレーション安全サブシステムとVDEコンテンツ制御情報参加者のVDEインストレーション安全サブシステムの経路との間のVDEインストレーション安全サブシステムによって管理された通信（例えば、少なくとも一部が暗号化された制御情報の配送者の認証を含む）を用いた安全な形態で提供され得る。この制御情報は、例えば、金融サービスプロバイダによって供給されるクレジットへのアクセス権、行政機関によって制定される規定または法律の施行、または顧客によって受け取られる使用情報の生成、取扱いおよび報告方法に関するVDEによって管理されたコンテンツ使用情報（そのような顧客以外の1つ以上のパーティによってコンテンツの使用を反映する）の顧客の要件に関連し得る。そのような制御情報は、たとえば、電子商取引に関連した法律のような社会的用件を強要し得る。

VDEコンテンツ制御情報は、コンテンツの異なる経路および制御情報取扱い参加者に異なって与えられ得る。さらに、VDE参加者がそのような行動をとることを許可された場合、パーミッション記録権利は、VDE参加者によって付加、変化および／または取り除かれ得る。VDE参加者の権利は、コンテンツおよび／またはコンテンツ制御情報（例えば、パーミッション記録）の取扱いのチェーンにおいて特定のパーティおよび／またはパーティのカテゴリーおよび／またはパーティの他のグループに関連して規定され得る。与えられた、資格のある単数のあるいは複数のパーティによって行われ得る制御情報の改変は、それらのパーティが行い得る改変の数、およびまたは改変の程度において制限され得る。

クリエータ、配布者、監査者、情報交換所、クライアント、管理者およびエンドユーザ（上記の分類の2つ以上が単一のユーザを記載し得ることを理解しつつ

）の電子機器における少なくとも1つの安全なサブシステムは、（意図されたアプリケーションに対して）以下のための「十分に」安全な環境を提供する。

1．プロパティおよび制御情報の復号化、

2．制御および計量に関連する情報の格納、

3．通信の管理、

4．VDE管理者の嗜好および要件の施行を含む、電子コンテンツおよび／または機器権利保護のための制御情報を構成するコア制御プログラムを、関連づけられたデータと共に処理すること。

通常、大半の使用、監査、報告、支払いおよび配布コントロールメソッド自体は、少なくとも一部が暗号化されたVDEインストレーションの安全なサブシステムによって実行される。従って、例えば、安全なサブシステム内で課金および計量記録は安全に生成および更新され得、暗号化および復号化鍵は安全に利用される。VDEはまた、VDE構成の参加者位置（ノード）安全サブシステム間に情報を通過させるとき、安全な（例えば、暗号化および認証された）通信を用いるので、VDE電子契約の重要はコンポーネントが、意図された商業目的のために十分なセキュリティをもって（十分に信頼されて）信頼性をもって施行され得る。価値チェーンについてのVDE電子契約は、少なくとも一部が、価値チェーン参加者の1つ以上のサブセット間での1つ以上の副契約（subagreement）からなり得る。これらの副契約は、VDE参加者の権利の保護を保証する1つ以上の電子契約「コンプライアンス」エレメント（関連づけられたパラメータデータを含むメソッド）からなる。

VDE構成の信頼性の程度は、参加者位置安全サブシステムでハードウェアSPUが用いられるかどうか、SPUハードウェアセキュリティアーキテクチャの有効性、SPUがソフトウェアにおいてエミュレートされるときのソフトウェアセキュリティ技術、およびコンテンツ、制御情報、通信およびVDEノード（VDEインストレーション）安全サブシステムへのアクセスを安全に行うために用いられる暗号化アルゴリズムおよび鍵に主に依存する。物理的機能およびユーザ識別認証セキュリティ手順は、そのようなセキュリティ手順がユーザノードでハードウェアSPUを用

いるVDE構成との信頼できる相互動作性に十分なセキュリティを提供し得る、確立された金融情報交換所などのあるノードにおいてハードウェアSPUの代わりに用いられ得る。

新しいまたは改変された制御情報を収容するための、VDE構成の各位置でのプロパティ管理ファイルの更新は、VDE安全サブシステム中で、保護下のサブシステムによって実行されるプログラムを更新する安全な管理ファイルの制御下で行われる。すべての安全な通信の少なくとも一部は暗号化され、安全なサブシステム内の処理が外部の観察および妨害から隠匿されるので、コンテンツ制御情報が施行され得ることが本発明によって保証される。その結果、クリエータおよび／または配布者および／またはクライアント管理者および／または各プロパティについての安全な制御情報の他の寄与者（例えば、報告し得る監査情報の種類を限定するエンドユーザ、および／または配布されたコンテンツの使用についての支払いのためのそのクレジットの使用についてある基準を確立する金融情報交換所）は、それらの寄与され許容された制御情報が（与えられたVDEセキュリティ実施設計のセキュリティ制限内で）施行されることを確信し得る。この制御情報は、例えば、以下を決定し得る。

（１）どのようにおよび／または誰に電子コンテンツが提供されるか、例えば、どのように電子プロパティが配布され得るか、

（２）１つ以上のオブジェクトおよび／またはプロパティ、またはオブジェクトまたはプロパティの一部がどのように、直接使用、例えば、復号化、表示、印刷などされ得るか、

（３）そのようなコンテンツおよび／コンテンツの一部の使用に対する支払いが、どのように取扱いされ得るか、あるいはされなければならないか、および、

（４）プロパティの少なくとも一部に関連する使用情報について監査情報がどのように収集、報告および／または使用されるか。

複数のパーティによって提出されたコンテンツ制御情報間の対立の解消を含む寄与された制御情報の上位性は、通常、以下によって確立される。

（１）様々なパーティによってインプレースに制御情報が置かれるシーケンス

（インプレース制御情報は、次に提出された制御情報に対して通常優位である）

、

（２）VDEコンテンツおよび／または機器制御情報の特定詳細。例えば、インプレース制御情報は、１つ以上のパーティまたはパーティのクラスからの制御の１つ以上の次の部分のいずれが、１つ以上のさらに異なるパーティおよびパーティのクラスによって提出される制御情報に対して優位になるかを規定し得る、

（３）どの制御情報が、VDE管理コンテンツの与えられた部分および／またはVDEインストレーションについての結果として得られる制御情報セットを構成するかを確立する、複数のパーティからの制御情報セット間のネゴシエーション。

電子契約および権利保護

VDEの重要な特徴は、VDEが、本発明の使用によって実行される電子契約のためのセキュリティおよび権利保護の管理および適切さを保証するために用いられることである。そのような契約には、以下の一つ以上が関わり得る。

（１）電子情報のクリエータ、出版社、および他の配布者、

（２）金融サービス（例えば、クレジット）プロバイダ、

（３）コンテンツ指定統計的情報およびユーザ指定記述情報などのコンテンツ使用から生じる情報の（サービスプロバイダ以外の）ユーザ。そのようなユーザは、市場分析、直接の指示された市場売買のための市場リストコンパイラ、および政府機関、

（４）コンテンツのエンドユーザ、

（５）それらのサービスおよび／または装置の使用に基づいて補償を受け取る遠隔通信会社およびハードウェア製造者（半導体および電子機器および／または他のコンピュータシステム製造者）などの下部構造サービスおよび装置プロバイダ、および

（６）電子情報によって記述されるあるパーティ、

を含み得る。

VDEは、商業的に安全な「拡張」価値チェーン電子契約をサポートする。VDEは、この拡張された契約を含むパーティ間の様々な基礎を成す契約をサポートする

ように構成され得る。これらの契約は、以下を含む重要な電子商取引に考慮されるものを規定し得る。

（１）セキュリテイ、

（２）電子配布を含むコンテンツ使用制御、

（３）プライバシー（例えば、医学的、クレジット、税金、個人的および／または他の形態の秘密情報によって記述されるパーティに関する情報に関する）、

（４）金融プロセスの管理、

（５）電子コンテンツ、コンテンツおよび／または機器制御情報、電子コンテンツおよび／または機器使用情報および支払いおよび／またはクレジットのための取扱い経路。

VDE契約は、価値チェーンの２つ以上のパーティの電子商取引関係を規定し得るが、そのような契約は、ときどき、他のVDE価値チェーン参加者を直接強制し、あるいは直接巻き込み得ない。例えば、コンテンツクリエータと配布者との間の電子契約は、クリエータのコンテンツに対する（VDEコンテナオブジェクト中に配布されたプロパティに対してなどの）配布者への価格、およびこの配布者が与えられた期間にエンドユーザに配布し得るこのオブジェクトのコピーの数の両方を規定し得る。第２の契約において、コンテンツ使用のための配布者請求の受容およびクリエータの著作権を保持することに同意するなどの配布された商品を用いるためのある要件にエンドユーザが同意する第３者契約に、価値チェーンエンドユーザが関連し得る。第３の契約は、配布者と、エンドユーザが、エンドユーザにクレジットを拡張する情報交換所と直接別の（第４の）契約を有する場合は、製品についての支払いのための情報交換所のクレジットを使用することを配布者に可能にする金融情報交換所との間に存在し得る。第５の発展する契約は、コンテンツ制御情報が取扱いのそのチェーンに沿って通過するに従って、すべての価値チェーン参加者間で進展し得る。この発展する契約は、例えば、各パーティによって受け取られる情報の性質およびコンテンツ使用情報および関連する手順の取扱い経路を含む、コンテンツ使用情報に対するすべてのパーティの権利を確立し得る。本実施例における第６の契約は、すべてのパーティを契約に関係さ

せ得、セキュリティ技術および信頼性の程度など（例えば、システムの商業的統合には、各VDEインストレーション安全サブシステムが、それらのVDEノードがある相互動作要件を満たすことを電子的に保証することを必要とする）のある一般的な仮定を確定する。上記の例において、これらの６つの契約は、この商業価値チェーン例についての拡張された契約の契約を含む。

VDE契約は、既にインプレースである制御情報と相互作用する新たに提案されたコンテンツ制御情報間の、非常に単純なものから精巧な「ネゴシエーション」までを介して現在のおよび／または新しい参加者によって、および／または複数のパーティによって提出された、同時に提案されたコンテンツ制御情報間のネゴシエーションによって改変され得る発展する（「生きている」）電子契約構成をサポートする。与えられたモデルは、既存の上位の規則に従って経時的に非同期的に漸次改変され得る。そのような改変は、全てに、特定のコンテンツ、および／またはクラスおよび／または特定のユーザおよび／またはユーザノードに、および／またはこれらのクラスに適用され得る。コンテンツの与えられた部分は、そのコンテンツ制御情報の発展に依存して（および／または、異なる適用可能なVDEインストレーションコンテンツ制御情報に依存して）異なる時間あるいは異なる取扱いに供され得る。制御情報の発展は、オブジェクトを含む１つ以上の制御情報に沿う通過の間に生じ得る。すなわち、制御情報は、改変が許容される限り、制御情報取扱いのチェーンに沿って１つ以上の点で改変され得る。その結果、VDEによって管理されるコンテンツは、コンテンツ取扱いのチェーンにおける異なる「位置」およびそのようなコンテンツの取扱いの異なるチェーンにおける同様の位置の両方において与えられる異なる制御情報を有し得る。また、制御情報のそのような異なるアプリケーションは、あるパーティあるいはパーティのグループが、別のパーティあるいはパーティのグループとは異なるコンテンツに供されることを指定するコンテンツ制御情報から得られ得る。例えば、コンテンツの与えられた部分についてのコンテンツ制御情報は上位情報として、従って、変更不可能な情報として規定され、コンテンツクリエータによってインプレースに置かれ、これらのコンテンツの与えられた部分の国内配布者は、コピーがbo

ni fideエンドユーザに供給される限り、３ヶ月毎に100000部のコピーを作成することが許可され得るが、そのようなコンテンツの単一のコピーのみを遠隔小売業者に受け渡し、制御情報は、そのような小売業者がエンドユーザへの小売りのためにコピーを毎月1000部を越えずに作成することを制限することを規定し得る。さらに、そのようなコンテンツのエンドユーザは、同一のコンテンツ制御情報によってそのようなコンテンツの３部のコピーを作成するように制限され、３部のコピーの各々は、エンドユーザが用いる３つの異なるコンピュータ（１つは仕事場のデスクトップコンピュータ、１つは家でのデスクトップコンピュータ、もう一つは携帯用コンピュータ）用である。

本発明の好ましい実施の形態によってサポートされる電子契約は、非常に単純なものから非常に精巧なものまで幅があり得る。これらの契約は、電子情報セキュリティ、使用管理、および通信を提供する非常に様々な情報管理モデル、および以下をサポートし得る。

（ａ）　情報、例えば、商業リテラルな(literary)プロパティの安全な電子配布、

（ｂ）　安全な電子情報使用モニタおよび報告、

（ｃ）　電子情報および／または機器使用および他の電子クレジットおよび／または通貨使用および管理ケーパビリティの両方に関連する安全な金融取引ケーパビリティ、

（ｄ）　ユーザが放出することを望まない使用情報のプライバシー保護、および、

（ｅ）　以下をフレキシブルに収容する「活動的」電子情報コンテンツ分散モデル、

（１）ある幅の参加者、

（２）コンテンツの取扱い、コンテンツおよび／または機器制御情報、コンテンツおよび／または機器使用関連情報の報告、および／または支払いのための１つ以上の経路（チェーン）、

（３）電子ネゴシエーションケーパビリティの使用を含むコンテンツ制御

情報に組み込まれる約定および条件の発展のサポート、

（４）新しいコンテンツ集合体を形成するための複数の部分のコンテンツの組み合わせのサポート、および、

（５）複数の並行モデル。

安全な処理ユニット

本発明によって提供されるVDEの重要な部分は、各ユーザのコンピュータ、他の電子機器あるいはネットワークに代表的に存在しなければならない、本明細書においてSPUと称されるコア安全取引制御構成である。SPUは、復号化鍵の生成、情報の暗号化および復号化、電子機器（すなわち、VDEインストレーション間および／または単一のVDEインストレーション内の複数のVDEインスタンスの間）の鍵および他の情報の安全な通信の管理、安全なおよび／非安全な不揮発性メモリ中の監査追跡、報告および予算作成情報の安全な累算および管理、制御情報管理命令の安全なデータベースの維持、およびある他の制御および管理上の機能を行うための安全な環境の提供のための信頼できる環境を提供する。

あるVDE活動を行うための信頼できる環境が要求される場合、VDEノード中のハードウェアSPU（ソフトウェアエミュレーションではない）が必要となる。そのような信頼できる環境は、電子機器内で用いられるための、および／または電子機器に動作可能に接続される、ある制御ソフトウェア、半導体あるいは半導体チップセットなどの１つ以上の不正改変不可能なハードウェアモジュール（例えば、不正改変不可能なハードウェア電子機器周辺装置）によって作り出され得る。本発明によって、ハードウェアSPUの信頼性は、そのハードウェアエレメントの一部あるいはすべてを不正改変不可能なパッケージング内に封入することによって、および／または他の不正改変不可能な技術（例えば、マイクロフュージョン(microfusing)および／または薄配線検出技術）を用いることによって高くされ得る。実施される本発明の信頼できる環境は、一部には、不正改変半導体設計の使用によって、マイクロプロセッサなどのVDEプロセスを安全に実行する制御論理を含む。

VDEノードのハードウェアSPUはVDE安全サブシステムのコアコンポーネントで

あり、マイクロコントローラ、マクロコンピュータ、または他のCPU構成などの電子機器の主要な制御論理の一部あるいはすべてを用い得る。あるいは、このような制御は、電子機器の非VDE機能の一部あるいはすべての制御などの非VDE目的に用いられ得る。ハードウェアSPUモードにおける動作時には、一次制御論理は、重要なVDEプロセスを保護および隠匿するように十分に安全でなければならない。例えば、ハードウェアSPUは、VDE関連活動を行うと同時に、従って、VDEプロセスの一部がある程度のセキュリティをもって実行することを可能にすると同時に、保護モードで動作するホスト電子機器マイクロコンピュータを用い得る。この別の実施の形態は、一次制御論理の一部ではない１つ以上の不正改変不可能な半導体の組み合わせを用いて信頼できる環境が作り出される好ましい実施の形態とは対照的である。いずれの実施の形態でも、ある制御情報（ソフトウェアおよびパラメータデータ）は、SPU内で安全に保持されなければならず、さらに制御情報は外部に安全に（例えば、暗号化されタグ付けされた形態で）格納され、必要なときは上記のハードウェアSPU内にロードされる。多くの場合において、特にマ

イクロコンピュータと共に用いるとき、上記の一次制御論理を用いるのではなく、上記VDEプロセスを実行するために特殊目的安全ハードウェアを用いる好ましい実施の形態のアプローチは、より安全で効率的であり得る。信頼できるSPUハードウェアプロセスに要求されるセキュリティおよび不正改変不可能性のレベルは、特定の市場または市場ニッチの商業的要件に依存し、広範なばらつきがあり得る。

図面の簡単な説明

本発明によって提供されるこれらのおよび他の特徴および利点は、図面に関連して現時点で好ましい実施例の実施の形態の以下の詳細な説明を参照することによって、よりよくおよびより完全に理解され得る。

図１は、本発明の好ましい実施例／実施の形態に従って提供される「仮想配布環境」の一例を示す。

図１Ａは、図１に示される「情報ユーティリティ」の一例をより詳細に示す図である。

図２は、処理および制御のチェーンの一例を示す。

図２Ａは、図２の処理および制御のチェーンにおいて一人の参加者から別の参加者へ規則および制御情報がどのように持続し得るかの一例を示す。

図３は、提供され得る異なる制御情報の一例を示す。

図４は、いくつかの異なるタイプの規則および／または制御情報の例を示す。

図5Aおよび図5Bは、「オブジェクト」の例を示す。

図６は、安全な処理ユニット（「SPU」）の一例を示す。

図７は、電子機器の一例を示す。

図８は、図７に示されている電子機器の一例のより詳細なブロック図である。

図９は、図６および図８に示されている安全な処理ユニット（「SPU」）の一例の詳細な図である。

図１０は、仮想配布環境によって提供される「権利オペレーティングシステム」（「ROS」）アーキテクチャの一例を示す。

図１１Ａ～図１１Ｃは、アプリケーションと権利オペレーティングシステムとの間の機能上の関係の例を示す図である。

図１１Ｄ～図１１Ｊは、「コンポーネント」および「コンポーネントアセンブリ」の例を示す。

図１２は、図１０に示される権利オペレーティングシステムの一例のより詳細な図である。

図１２Ａは、どのように「オブジェクト」が作成されるかの一例を示す。

図１３は、図１２に示される「プロテクト下の処理環境」のためのソフトウェアアーキテクチャの一例の詳細なブロック図である。

図１４Ａ～図１４Ｃは、図１３に示されるプロテクト下の処理環境によって提供されるSPUメモリマップの例である。

図15は、図１３のチャネルサービスマネジャおよびロードモジュール実行マネージャがチャネルをどのようにサポートし得るかの一例を示す。

図15Aは、図15に示されるチャネルヘッダおよびチャネル詳細レコードの一例である。

図15Bは、チャネルを形成するために図１３のプロテクト下の処理環境によって行われ得るプログラム制御ステップの一例のフローチャートである。

図１６は、安全なデータベース構造の一例のブロック図である。

図１７は、論理オブジェクト構造の一例の図である。

図１８は、静止オブジェクト構造の一例を示す。

図１９は、移動オブジェクト構造の一例を示す。

図２０は、コンテンツオブジェクト構造の一例を示す。

図２１は、管理的オブジェクト構造の一例を示す。

図２２は、メソッドコア構造の一例を示す。

図２３は、ロードモジュール構造の一例を示す。

図２４は、ユーザデータエレメント（ＵＤＥ）および／またはメソッドデータエレメント（ＭＤＥ）構造の一例を示す。

図25A～図２５Ｃは、「マップ計量」の例を示す。

図２６は、パーミッションレコード（ＰＥＲＣ）構造の一例を示す。

図２６Ａおよび図２６Ｂは共に、パーミッションレコード構造のより詳細な例を示す。

図２７は、発送（shipping）テーブル構造の一例を示す。

図２８は、受信テーブル構造の一例を示す。

図２９は、管理的イベントログ構造の一例を示す。

図３０は、図１６の安全なデータベース中に示されるオブジェクト登録テーブル、サブジェクトテーブル、およびユーザ権利テーブル間の相互関係および使用の例を示す。

図３１は、図１６に示されるオブジェクト登録テーブルのより詳細な例である。

図３２は、図１６に示されるサブジェクトテーブルのより詳細な例である。

図３３は、図１６に示されるユーザ権利テーブルのより詳細な例である。

図３４は、サイト記録テーブルおよびグループ記録テーブルが図１６に示される安全なデータベースの部分をどのようにトラッキングし得るかの指定例を示す。

図３４Ａは、図３４のサイトレコードテーブル構造の一例である。

図３４Ｂは、図３４のグループレコードテーブル構造の一例である。

図３５は、安全データベースを更新するためのプロセスの一例を示す。

図３６は、新しいエレメントがどのように図１６の安全なデータベースに挿入され得るかの一例を示す。

図３７は、安全なデータベースのエレメントがどのようにアクセスされ得るかの一例を示す。

図３８は、安全なデータベースエレメントをどのように保護するかのフローチャート例である。

図３９は、安全なデータベースをどのようにバックアップするかのフローチャート例である。

図４０は、バックアップからどのように安全データベースを回復するかのフローチャート例である。

図４１Ａ～図４１Ｄは、「相互的メソッド」を用いてどのように「処理および制御チェーン」が使用可能にされ得るかを示す一組の例である。

図４２Ａ～図４２Ｄは、「相互的」BUDGETメソッドの一例を示す。

図４３Ａ～図４３Ｄは、「相互的」REGISTERメソッドの一例を示す。

図４４Ａ～図４４Ｃは、「相互的」AUDITメソッドの一例を示す。

図４５～図４８は、コンテンツまたは他の情報の放出を制御するために共に用いられる幾つかのメソッドの例を示す。

図４９、図４９Ａ～図４９Ｆは、OPENメソッドの一例を示す。

図５０、図５０Ａ～図５０Ｆは、READメソッドの一例を示す。

図５１、図５１Ａ～図５１Ｆは、WRITEメソッドの一例を示す。

図５２は、CLOSEメソッドの一例を示す。

図５３Ａおよび図５３Ｂは、EVENTメソッドの一例を示す。

図５３Ｃは、BILLINGメソッドの一例を示す。

図５４は、ACCESSメソッドの一例を示す。

図55A～図55Bは、DECRYPTおよびENCRYPTメソッドの例を示す。

図５６は、CONTENTメソッドの一例を示す。

図５７Ａおよび図５７Ｂは、EXTRACTおよびEMBEDメソッドの例を示す。

図５８Ａは、OBSCUREメソッドの一例を示す。

図５８Ｂ、５８Ｃは、FINGERPRINTメソッドの例を示す。

図５９は、DESTROYメソッドの一例を示す。

図６０は、PANICメソッドの一例を示す。

図６１は、METERメソッドの一例を示す。

図６２は、鍵「旋回（convolution）」プロセスの一例を示す。

図６３は、「真の」鍵を決定するための鍵旋回プロセスを用いてどのように異なる鍵が生成され得るかの一例を示す。

図６４および図６５は、保護下の処理環境鍵がどのように初期化されるかの一例を示す。

図６６および図６７は、静止オブジェクトおよび移動オブジェクト内にそれぞれ含まれる情報を復号化するためのプロセスの例を示す。

図６８は、保護下の処理環境がどのように初期化され得るかの一例を示す。

図６９は、ファームウェアが保護下の処理環境にどのようにダウンロードされ得るかの一例を示す。

図７０は、ネットワークあるいは他の通信手段と共に接続された複数のVDE電子機器の例を示す。

図７１は、携帯VDE電子機器の例を示す。

図７２Ａ～図７２Ｄは、ユーザ通知および例外（exception）インタフェースによって生成され得る「ポップアップ」ディスプレイの例を示す。

図７３は、「スマートオブジェクト」の一例を示す。

図７４は、「スマートオブジェクト」を用いるプロセスの一例を示す。

図75A～図７５Ｄは、電子ネゴシエーションのために用いられるデータ構造の

例を示す。

図７５Ｅ～７５Ｆは、電子契約に関連する構造の例を示す。

図７６Ａ～図７６Ｂは、電子ネゴシエーションプロセスの例を示す。

図７７は、取扱いおよび制御のチェーンの別の例を示す。

図７８は、ＶＤＥ「格納場所（repository）」の一例を示す。

図７９～図８３は、ＶＤＥ管理コンテンツおよび制御情報を発展および変形させるための処理および制御のチェーンを図示する例を示す。

図８４は、ＶＤＥ参加者のいくつかのカテゴリーに関する処理および制御のチェーンの別の例を示す。

図８５は、組織内の配布および処理のチェーンの別の例を示す。

図８６および図８６Ａは、処理および制御のチェーンの別の例を示す。

図８７は、仮想シリコンコンテナモデルの例を示す。

より詳細な説明

図１～図７および以下の検討は、本発明によって提供される特徴のいくつかの局面の概要を示す。本発明による実施の形態のより技術的な「詳細な説明」が、この概要の後に示される。

概要

図１は、本発明に従って提供され得る「仮想配布環境」（「ＶＤＥ」）１００を示す。図１において、情報ユーティリティ２００は、例えば、電話あるいはケーブルＴＶラインなどの通信手段２０２に接続する。電話あるいはケーブルＴＶライン２０２は、電子情報を場所から場所へ運搬する「電子ハイウエイ」の一部であり得る。ライン２０２は、情報ユーティリティ２００を、例えば、消費者２０８、オフィス２１０、ビデオ製作スタジオ２０４および出版社２１４などの他の人々に接続する。情報ユーティリティ２００に接続される人々は仮想配布環境１００内で生じる取引に参加し得るので、各々が「ＶＤＥ参加者」と称され得る。

考えられ得るほぼすべての種類の取引が、仮想配布環境１００によってサポートされ得る。仮想配布環境１００によってサポートされ得る取引の多くの例のいくつかには、以下が含まれる：

C　ホームバンキングおよび電子支払い；

C　電子法的契約；

C　電子印刷物、映像、音声、イメージおよびコンピュータプログラムなどの「コンテンツ」の配布；および

C　医学記録および金融情報などの秘密情報の安全な通信。

仮想配布環境100は、権利を保護し、信頼性があり予測可能な配布を保証し、かつ、コンテンツクリエータおよび配布者に対する適切な補償を保証するために必要なものとして用いられる多くの物理的な「物」を要求しないので、「仮想」である。例えば、過去には、情報はコピーが困難であったレコードあるいはディスク上で配布された。過去には、秘密あるいは秘密コンテンツは、特使によって配送される封をされた封筒あるいはロックされたブリーフケースに入れられて配布された。適切な補償を保証するために、消費者は販売人に現金を渡した後にしか商品およびサービスを受け取れなかった。情報ユーティリティ200は、電子記録媒体などの物理的な「物」を移動させることによって情報を配送し得るが、仮想配布環境100は完全に電子的な「処理および制御のチェーン」を促進させる。

VDEフレキシビリティによる取引のサポート

情報ユーティリテイ200は、多くの異なる種類の情報取引をフレキシブルにサポートする。異なるVDE参加者は、取引の異なる部分を規定し、および／またはそれに参加し得る。情報ユーティリティ200は、取引に関する情報の配送を補助してもよいし、あるいは取引参加者の一つであってもよい。

例えば、図1の右上角のビデオ製作スタジオ204は、ビデオ／テレビプログラムを製作し得る。ビデオ製作スタジオ204は、これらのプログラムをライン202を通って送ってもよく、衛星リンク205およびCD ROM配送サービス216などの他の経路を用いてもよい。ビデオ製作スタジオ204は、プログラムを消費者206、208および210に直接送り得る。あるいは、ビデオ製作スタジオは、例えば、情報ユーティリティ200にプログラムを送り、プログラムをそこに格納し、その後にプログラムを消費者に送り得る。すなわち、ビデオ製作スタジオあるいは情報ユーティリティ200が、プログラムを使用する権利を消費者に与える適切な「規則およ

び制御」（制御情報）を有するようにこれらの消費者をアレンジすると仮定すると、消費者206、208、210の各々は、ビデオ製作スタジオ204によって製作されたプログラムを受け取り、使用することができる。

消費者がビデオプログラムのコピーを有していても、消費者がプログラムの使用を承認する「規則および制御」を有さない限り、プログラムを見たりコピーしたすることはできない。消費者は、「規則および制御」によって許可されるようにしかプログラムを使用し得ない。

例えば、ビデオ製作スタジオ204は、できるだけ多くの視聴者が見ることを希望して30分の試用ビデオを放送し得る。ビデオ製作スタジオ204は、放送毎に2.00ドルを受け取ることを望む。ビデオ製作スタジオ204は、情報ユーティリティを介して、すべての消費者206、208、210に対して試用ビデオを「保護された」形態で利用可能にし得る。ビデオ製作スタジオ204はまた、ビデオに「規則および制御」も与え得る。これらの「規則および制御」は、例えば、以下を指定し得る：

（１）独立した金融プロバイダ212（MastercardまたはVISAなど）のクレジットアカウントに基づいて少なくとも2.00ドルの十分な（good）クレジットを有する消費者は誰でもビデオを見てもよい、

（２）仮想配布環境100は、消費者がビデオを見る毎に「計量し」、時折ビデオ製作スタジオ204に使用を報告する、および

（３）金融プロバイダ212は、ビデオを見る各消費者のクレジットアカウントから支払い（2.00ドル）を電子的に徴収し、これらの支払いをビデオ製作スタジオ204に振替し得る。

情報ユーティリティ200によって、小さいビデオ製作スタジオでも消費者にビデオを売り、その労力に対する補償を受け取ることが可能になる。さらに、ビデオ製作スタジオへの適切な支払いを行えば、価値を付加し、および／または再パッケージ者または再配布者となり得る他のビデオ製作会社に、ビデオが利用可能になり得る。

図１は出版社214も示している。出版社214は、著者206のための配布者となり

得る。出版社214は、「コンテンツ」（コンピュータソフトウェア、電子新聞、出版社214によって製作されたビデオ、音声あるいは他のいずれものデータ）を使用する権利を、オフィス210などの消費者に配布し得る。使用権は、出版社216によって配布される「規則および制御」によって規定され得る。出版社216は、これらの「規則および制御」をコンテンツと共に配布するが、これは必要なことではない。コンテンツは適切な「規則および制御」を有する消費者によってのみ使用され得るので、コンテンツおよびそれに関連する「規則および制御」は、異なる時間に異なる方法で異なるVDE参加者によって配布され得る。規則および制御が適用されるコンテンツとは別に、「規則および制御」を安全に配布し施行するVDEの能力は、大きな利点を提供する。

出版社214によって配布される権利を用いることによって、オフィス210が、例えば、コンテンツのコピーを製作し、それを従業員に配布することが可能になる。オフィス210は、「処理および制御のチェーン」を従業員まで拡張することによって再配布者となり得る。オフィス210は「規則および制御」（出版社214から受け取る「規則および制御」と一致する）を付加あるいは改変して、オフィス内部制御情報およびメカニズムを提供し得る。例えば、オフィス210は、オフィス内の各個人ユーザおよび／またはグループのための最大使用予算を設定してもよく、指定された従業員および／またはグループにある情報へのアクセスを許可してもよい。

図１は、消費者206に「CD ROM」ディスクなどの電子記憶媒体を消費者206に配送する情報配送サービス216も示している。電子記憶媒体自体はライン202を通って情報ユーティリティ200によって電子的に配送されないが、仮想配布環境100の一部のままである。電子記憶媒体は、コンテンツ、「規則および制御」あるいは他の情報を配布するために用いられ得る。

情報ユーティリティ200の内にあるものの例

図１における「情報ユーティリティ」200は、配布者、金融情報交換所、および管理者として働き得る参加者の集合であり得る。図１Ａは、情報ユーティリティ200の一例の内部にあり得るものの例を示している。情報ユーティリティ参加

者200a～200gは、各々が独立した組織／企業であり得る。各参加者200a～200gは、それぞれいくつ存在してもよい。本実施例においては、電子「スイッチ」200aは、情報ユーティリティ200の内部構成要素を互いにおよび外部の参加者と接続する。また、電子スイッチは、外部参加者を互いに接続してもよい。

情報ユーティリティ200は、参加者および／またはレポート受け取り者200eからの要求に基づいて取引（例えば、電子資金の振替のため）を処理する「取引プロセッサ」200bを含んでいてもよい。また、報告された使用情報を分析する「使用分析者」200cを含んでいてもよい。「レポート作成者」200dは、例えば、使用に基づいてレポートを作成してもよいし、外部参加者および／または情報ユーティリティ200内の参加者にこれらのレポートを提供してもよい。「レポート受け取り者」200eは、コンテンツユーザからの使用レポートなどのレポートを受け取り得る。「パーミッションエージェント」200fは、例えば、消費者のクレジット価値のプロフィールに基づいて、使用あるいは配布パーミッションを与える「規則および制御」を配布し得る。管理者200hは、仮想配布環境100の適切な動作を維持する情報を提供し得る。コンテンツおよびメッセージ記憶装置200gは、情報ユーティリティ200内あるいは外部の参加者によって使用される情報を格納し得る。

「処理および制御のチェーン」を用いた「コンテンツ」の配布の例

上記で説明したように、仮想配布環境100は、ほぼすべての種類の取引を管理するために用いられ得る。管理のために仮想配布環境100が用いられ得る重要な取引のタイプの一つには、「コンテンツ」あるいは他の重要な情報の配布あるいは通信がある。図２は、図１の仮想配布環境100がコンテンツを配布するための「処理および制御のチェーン」を提供するためにどのように用いられ得るかの「モデル」をより抽象的に示している。図２の各ブロックは、図１に示されている１つ以上のVDE参加者に対応し得る。

図２の例において、VDEコンテンツクリエータ102は、コンテンツを作成する。コンテンツクリエータ102はまた、コンテンツを配布するための「規則および制御」を指定し得る。これらの配布に関連する「規則および制御」は、コンテンツ

を使用するための権利を配布するパーミッションを有する人物およびコンテンツ使用を許可された人数を指定し得る。

矢印104は、コンテンツに関連付けられた「規則および制御」を電子ハイウエイ108を通って（あるいは米国郵便などの配送サービスによって送られる光ディスクなどの他の経路によって）VDE権利配布者106（「配布者」）に送るコンテンツクリエータ102を示している。コンテンツは、「規則および制御」を送るために用いられたものと同一のあるいは異なる経路を通って配布され得る。配布者106は、コンテンツの使用に関連する自分自身の「規則および制御」を作る。使用に関連する「規則および制御」は、例えば、コンテンツを用いてユーザができることおよびできないこと、ならびにコンテンツを使用するためにかかる費用を指定し得る。これらの使用に関連する「規則および制御」は、コンテンツクリエータ102によって指定される「規則および制御」と一致しなければならない。

矢印110は、コンテンツの「規則および制御」を消費者などのコンテンツユーザ112に送ることによってコンテンツを使用する権利を配布する配布者106を示している。コンテンツユーザ112は、使用に関連する「規則および制御」に従ってコンテンツを用いる。

この図２の例において、コンテンツ使用に関する情報は、矢印114によって示されるように、金融情報交換所116に報告される。この「報告」に基づいて、金融情報交換所116は請求書を作り、その請求書を「レポートおよび支払い」ネットワーク118を通ってコンテンツユーザ112に送り得る。矢印120は、内容使用に対する支払いを金融情報交換所116に行うコンテンツユーザ112を示している。受け取るレポートおよび支払いに基づいて、金融情報交換所116は配布者にレポートおよび／または支払いを与え得る。配布者106は、矢印122が示すように、コンテンツクリエータ102へレポートおよび／または支払いを与え得る。金融情報交換所116は、クリエータ102にレポートおよび支払いを直接与え得る。報告および／または支払いは、異なるように行われ得る。例えば、情報交換所116は、直接あるいはエージェントを介して、VDEコンテンツクリエータ102および権利配布者106の各々にレポートおよび／または支払いを与え、ならびにコンテンツユーザ1

１２にレポートを与え得る。

配布者１０６およびコンテンツクリエータ１０２は、同一人物でも、異なる人物でもよい。例えば、音楽活動を行うグループは、自分自身の音楽レコーディングを行い配布することによって、コンテンツクリエータ１０２および配布者１０６の両方となり得る。別の例として、出版社は、著者であるコンテンツクリエータ１０２によって作成された作品を使用する権利を配布する配布者１０６となり得る。コンテンツクリエータ１０２は、コンテンツ配布の金融目的を効率的に管理するために配布者１０６を用い得る。

図２に示される「金融情報交換所」１１６は、「VDE管理者」でもあり得る。VDE管理者の役割を行う金融情報交換所１１６は、「管理」情報をVDE参加者に送る。この管理上の情報によって、仮想配布環境１００の適切な動作が維持され得る。「VDE管理者」および金融情報交換所の役割は、異なる人あるいは会社によって行われ得る。また、これらは各々１つを越える数であり得る。

さらに「規則および制御」について

仮想配布環境１００は、「規則および制御」（制御情報）によって許可されるときを除いて、保護下の情報の使用を防止する。例えば、図２に示される「規則および制御」はあるコンテンツを使用する「パーミッション」をコンテンツユーザ１１２の特定の個人あるいはクラスに与え得る。これらの規則および制御は、どの種類のコンテンツ使用が許可され、どの種類が許可されないかを指定し得る。これらの規則および制御は、コンテンツ使用に対する支払い方法、およびそれにかかる費用を指定し得る。別の例として、「規則および制御」は、再び配布者１０６および／またはコンテンツクリエータ１０２にコンテンツ使用情報を報告することを必要とし得る。

「処理および制御のチェーン」の各VDE参加者は、通常は「規則および制御」を受ける。「規則および制御」は、様々なVDE参加者の各々のそれぞれの権利および義務を規定する。「規則および制御」は、参加者間の相互依存性および関係を確立し得る情報およびメカニズムを提供する。「規則および制御」はフレキシブルであり、「仮想配布環境」１００が大半の「従来の」企業取引をサポートする

こ.とを許可する。例えば、

C　「規則および制御」は、金融情報交換所116がどの支払いを処理し得るかを指定し得る。

C　「規則および制御」は、参加者がどの種類の使用情報を受け取るかを指定し得る。および

C　「規則および制御」は、ある情報が一部の参加者にさらされ(reveal)、他の情報はそれらの参加者には秘密にされることを指定し得る。

「規則および制御」は、それらが変更され得るか否か、およびどのように変更され得るかを自己制限し得る。しばしば、ある１人のVDE参加者によって指定される「規則および制御」は、他のVDE参加者によって変更され得ない。例えば、コンテンツユーザ112は、一般的に、ユーザがある料金をコンテンツ使用に対して支払うことを要求する配布者106によって指定される「規則および制御」を変更し得ない。「規則および制御」は「処理および制御のチェーン」を通って渡されるときに「持続」し、あるVDE参加者から次の参加者に渡されるときに「引き継がれ」得る。

要求に基づいて、VDE参加者は、それらの参加者の「規則および制御」が同一のあるいは別の「規則および制御」によって指定される条件で変更され得ることを指定し得る。例えば、コンテンツクリエータ102によって指定される「規則および制御」は、まさに小売店が商品の卸売り価格に「上乗せ」するように、配布者106が使用価格に「上乗せ」するのを許可し得る。図２Ａは、ある「規則および制御」がコンテンツクリエータ102からコンテンツユーザ112に変化しない状態で持続し、別の「規則および制御」は配布者106によって改変あるいは削除され、さらに別の「規則および制御」が配布者によって付加される例を示している。

「規則および制御」は、他のVDE参加者に報告される情報を制限することによってコンテンツユーザのプライバシーを保護するために用いられ得る。一例として、「規則および制御」は、コンテンツユーザのアイデンティティを明らかにせずに、コンテンツ使用情報を匿名で報告させ得る。あるいは、「規則および制御」は、必要である場合は、「適切なパーミッション」を用いてある参加者へある情報（例えば、使用から得られた情報）のみを知らせ得る。どの情報が知らさ

れ、その情報がどのVDE参加者に知らされるかを安全に制御するこの能力によって、すべてのVDE参加者のプライバシー権が保護されることが可能になる。

別々に配送され得る「規則およびコンテンツ」

上述のように、仮想配布環境100は、コンテンツを対応する「規則および制御」と関連づけ、対応する「規則および制御」のセットが利用可能にならない限り、コンテンツが使用あるいはアクセスされることを防止する。配布者106は、コンテンツの配布を制御するためにコンテンツを配送する必要がない。好ましい実施の形態は、非許可配布および使用から「許可および制御」を可能にする対応する使用を保護することによって、コンテンツを安全に保護し得る。

いくつかの例では、「規則および制御」は、それらが適用されるコンテンツと共に移動し得る。仮想配布環境100によって、「規則および制御」がコンテンツとは別に配送されることも可能になる。対応する「規則および制御」からの「パーミッション」がなければ保護下のコンテンツを誰も使用できず、あるいはコンテンツにアクセスし得ないので、配送者106は既に配送された（あるいは将来配送される）コンテンツの使用を制御し得る。「規則および制御」は、コンテンツ配送に用いられるものとは異なる経路を通って配送され得る。「規則および制御」もまた、別の時間に配送され得る。コンテンツクリエータ102は、電子ハイウエイ108を通ってコンテンツユーザ112にコンテンツを配送し得る。あるいは、コンテンツクリエータは、コンテンツをハイウエイ上で誰にでも利用可能にし得る。コンテンツは、配送時に用いられても、後の使用あるいは再使用のために格納されてもよい。

仮想配布環境100はまた、支払いおよびレポート手段を別々に配送することを可能にする。例えば、コンテンツユーザ112は、いずれものコンテンツの使用に対する支払いを行うためにクレジットを（ある制限まで）拡張する仮想「クレジットカード」を有し得る。「クレジット取引」は、「オンライン」接続あるいはさらなる承認をいずれも必要とせずに、ユーザのサイトで生じ得る。本発明は、仮想「クレジットカード」の非許可使用からの安全な保護を補助するために用いられ得る。

「規則およびコンテンツ」はプロセスを規定する

図３は、「規則および制御」に基づく全プロセスの例を示す。この例は、「イベント」プロセス402と、計量プロセス404と、課金プロセス406と、予算プロセス408とを含む。図３に示されるすべてのプロセスが、「規則および制御」の各セットについて用いられるわけではない。

「イベントプロセス」402は、生じたもの（「イベント」）を検出し、これらの「イベント」のいずれが他の「プロセス」による行動を必要とするかを決定する。「イベント」は、例えば、コンテンツを使用するためまたは使用パーミッションを出すための要求を含む。いくつかのイベントは付加的な処理を必要とし得るが、他のイベントは必要とし得ない。「イベント」がさらなる処理を必要とするか否かは、コンテンツに対応する「規則および制御」に依存する。例えば、パーミッションを欠くユーザは、自分の要求を満足させない（「No Go」）。別の例として、電子ブックの新しいページを開くための各ユーザ要求は満たされ得るが（「Go」）、これらの要求は計量、課金あるいは予算作成するためにはなくてもよい。小説を一部購入したユーザは、さらなる計量、課金または予算作成を行わずに、ユーザが望む回数だけ小説を開いて読むことを許可され得る。この単純な例において、「イベントプロセス」402は、ユーザが保護下の小説を初めて開きたいと思ったときに（すなわち、購入価格がユーザに請求され得るときに）計量、課金、および／または予算作成プロセスを要求し、後のすべての同一の小説を開くための要求を「重要ではないイベント」として取扱い得る。別のコンテンツ（例えば、電子電話帳のサーチ）は、アクセス毎に料金を支払うことをユーザに要求し得る。

「計量」プロセス404はイベントの記録をとり、配布者106および／または他の適切なVDE参加者に使用を報告し得る。図４は、以下のような複数の異なる因子にプロセス404が基づき得ることを示している。

（ａ）請求される使用のタイプ

（ｂ）請求が基づくユニットの種類、

（ｃ）ユニット毎の請求料金、

（ｄ）報告を行う時期、

（ｅ）支払い方法。

これらの要素は、計量プロセスを制御する「規則および制御」によって指定され得る。

課金プロセス406は、イベントついての請求額を決定する。このプロセスは、支払い情報を記録および報告する。

予算作成プロセス408は、許可されるコンテンツ使用量を制限する。例えば、予算作成プロセス408は、コンテンツがアクセスあるいはコピーされ得る回数を制限してもよいし、例えば、クレジットアカウントにおいて利用可能なドル金額に基づいて用いられ得るページ数あるいは他のコンテンツの量を制限してもよい。予算作成プロセス408は、そのような制限と関連づけられる金融および他の取引情報を記録および報告する。

これらのプロセスの実行が成功すると、コンテンツがユーザに供給され得る。

コンテナおよび「オブジェクト」

図5Aは、好ましい実施の形態において、情報の「規則および制御」によって与えられるとき以外に情報がアクセスされ得ないように、仮想配布環境100が情報エレメント（コンテンツ）を「コンテナ」302にどのようにパッケージし得るかを示している。通常は、コンテナ302は、物理的ではなく電子的である。１つの実施例における電子コンテナ302は、明確に規定された構造を有する「ディジタル」情報を含む。コンテナ302およびそのコンテンツは、「オブジェクト300」と称され得る。

図5Aの実施例は、コンテナ302「内」に入れられるアイテムを示している。しかし、コンテナ302は、これらのアイテムを実際にコンテナ内に格納せずに、アイテムを「含み」得る。例えば、コンテナ302は、遠隔サイト（site）の他のコンテナ中などの他の位置で利用可能なアイテムを参照し得る。コンテナ302は、異なる時間または制限された時間の間のみに利用可能なアイテムを参照し得る。アイテムには大きすぎてコンテナ302内に格納され得ないものもあり得る。アイテムは、例えば、ある時間での映像の「ライブ供給（live feed）」の形態でユ

ーザに配送され得る。その時でも、本実施例において、コンテナ302は（参照によって）ライブ供給を「含む」。

コンテナ302は、電子（「ディジタル」など）形態で情報コンテンツ304を含み得る。情報コンテンツ304は、小説のテキスト、写真、音楽演奏あるいは朗読などの音声、映画あるいは他のビデオ、コンピュータソフトウエア、あるいは考えられ得る他のほぼあらゆる種類の電子情報などであり得る。他のタイプの「オブジェクト」300（「管理オブジェクト」）は、情報コンテンツ304の代わりあるいはそれに加えて「管理上の」あるいは他の情報を含み得る。

図5Aの例において、コンテナ302は以下の形態の「規則および制御」も含み得る。

（ａ）「パーミッション記録」808

（ｂ）「予算」308、および

（ｃ）「他のメソッド」1000。

図5Bは、パーミッション記録808、予算308および他のメソッド1000に関していくつかの付加的な詳細を示す。「パーミッション記録」808は、例えば、コンテナ302を開けることができる人、オブジェクトのコンテンツを使用できる人、オブジェクトを配布し得る人、およびアクティブでなければならない他の制御メカニズムなどの、オブジェクト300に関連する権利を指定する。例えば、パーミッション記録808は、コンテナ302およびそのコンテンツを使用、配布および／または管理するユーザの権利を指定し得る。パーミッション記録808はまた、予算308および「他のメソッド」1000によって適用される要件も指定し得る。パーミッション記録808は、スクランブリングおよびデスクランブリング「鍵」などのセキュリティ関連情報も含み得る。

図5Bに示される「予算」308は、とりわけ、情報コンテンツ304の使用への制限、および使用に対する支払いがどのようになされるかを指定し得る、特別のタイプの「メソッド」1000である。予算308は、例えば、情報コンテンツ304全体のどの程度が用いられおよび／コピーされ得るかを指定し得る。メソッド３１０は、特定の予算によって指定される量を越える量の使用を防止し得る。

「他のメソッド」1000は、「規則および制御」によって用いられる基本的な動

作を規定する。そのような「メソッド」1000は、例えば、使用がどのように「計量」されるか、コンテンツ304および他の情報がスクランブルおよびデスクランブルされるか否かおよびどのようにスクランブルおよびデスクランブルされるか、および情報コンテンツ304の取扱いおよび制御に関連する他のプロセスを含み得る。例えば、メソッド1000は、電子コンテナ302を開けるすべての人のアイデンティティを記録し得、「計量」に基づいて情報内容がどのように請求がされるかを制御し得る。メソッド1000は、１つあるいは複数の異なる情報コンテンツ304および関連するコンテナ302、ならびに情報コンテンツ304のすべてのあるいは特定の部分に当てはまり得る。

安全な処理ユニット（SPU）

「VDE参加者」は各々「電子機器」を有し得る。機器はコンピュータであってもよいし、コンピュータを含んでいてもよい。機器は、電子ハイウエイ108を通って通信し得る。図６は、各VDE参加者によって本実施例で用いられる「電子機器」の安全な処理ユニット（「SPU」）500の部分を示している。SPU500は、安全な処理環境503において情報を処理し、重要な情報を安全に格納する。SPUは、ホスト電子機器において動作するソフトウェアによってエミュレートされ得る。

SPU500は、「不正改変不可能なセキュリティバリア」502中に封入され保護される。セキュリティバリア502は、他の領域から安全な環境503を分離する。これによって、安全な環境503内の情報およびプロセスが観察され、干渉され、適切な安全な条件下以外に置くことを防止する。バリア502はまた、SPU500内の安全なリソース、プロセスおよび情報への外部アクセスを制御する。１つの実施例において、不正改変不可能なセキュリティバリア502は、「暗号化」、ならびに不正改変を検出し、および／または不正改変が検出されると安全な環境503内の影響を受けやすい（sensitive）情報を破壊するハードウェアなどのセキュリティ特徴によって形成される。

本実施例におけるSPU500は、「ハードウェア」506および「ファームウェア」508を含む集積回路（「IC」）「チップ」504である。SPU500は、「機器リンク」510を介して電子機器の残りの部分と接続する。本実施例におけるSPU「ファーム

ウェア」508は、チップ504に「埋め込まれた」「コンピュータプログラム」などの「ソフトウェア」である。ファームウェア508は、ハードウェア506を動作させる。ハードウェア506は、好ましくは、ファームウェア508によって指定される命令を行うためのプロセッサを含む。「ハードウェア」506はまた、情報が不正改変され得ないように情報を安全に格納するための長期メモリおよび短期メモリを含む。SPU500はまた、イベントの時間を決定するために用いられる保護下のクロック／カレンダーも有し得る。本実施例におけるSPUハードウェア506は、あるプロセス（「暗号化」および「復号化」など）を迅速かつ効率的に行うように特別に設計された特殊目的電子回路を含み得る。

SPU500が用いられている特別なコンテクストは、SPU500がどの程度の処理能力を有するべきかを決定する。本実施例において、SPUハードウェア506は、図３に示されるプロセスの安全な部分をサポートするために十分な処理能力を少なくとも提供する。いくつかのコンテクストにおいて、SPU500の機能は、SPUがすべての電子機器処理を行い、汎用プロセッサに組み込まれ得るように向上され得る。別のコンテクストにおいて、SPU500は汎用プロセッサと共に作動し得るので、安全なプロセスを取り扱うために十分な処理能力のみを必要とする。

VDE電子機器および「権利オペレーティングシステム」

図７は、SPU500を含む電子機器600の一例を示す。電子機器600は、実質的に以下のようなどのような種類の電気装置あるいは電子装置であってもよい。

C　コンピュータ

C　ＴＶ「セットトップ」コントロールボックス、

C　ページャ

C　電話

C　サウンドシステム

C　ビデオ再生システム

C　ビデオゲームプレーヤ

C　「スマート」クレジットカード

である。

本実施例における電子機器600は、キーボードあるいはキーパッド612、音声認識器613、およびディスプレイ614を含み得る。人であるユーザは、キーボード612および／または音声認識器613を介してコマンドを入力することができ、ディスプレイ614上の情報を見得る。機器600は、電子機器内で通常用いられるいずれもの接続／機器を介して外界と通信し得る。図の底部に沿って示される接続／装置は以下のような例である：

「モデム」618または他の遠隔通信リンク；

CD ROMディスク620、あるいは他の記憶媒体または装置；

プリンタ622；

放送受信器624；

文書スキャナ626；および

「ネットワーク」に機器を接続する「ケーブル」628。

仮想配布環境100は、それらのハードウェアリソースを制御することによって機器600およびSPU500を管理する「権利オペレーティングシステム」602を提供する。オペレーティングシステム602はまた、少なくとも一つの「機器」608をサポートし得る。概して、「アプリケーション」608は、機器600のコンテクストに特定的なハードウェアおよび／またはソフトウェアである。例えば、機器600がパーソナルコンピュータである場合、「アプリケーション」608は、例えば、ワードプロセッサ、通信システムあるいはサウンドレコーダなどの、ユーザによってロードされるプログラムであり得る。機器600がテレビコントローラボックスである場合、アプリケーション608は、要求されるビデオをユーザが注文し、早送りおよび巻き戻しなどの他の機能を行うことを可能にするハードウェアまたはソフトウェアであり得る。本実施例において、オペレーティングシステム602は、多くの異なる「アプリケーション」608を用いてサポートおよび作動し得る、基準化され明確に規定され総合された「インタフェース」を提供する。

本実施例におけるオペレーティングシステム602は、「権利および監査オペレーティングシステム機能」604および「他のオペレーティングシステム機能」606を提供する。「権利および監査オペレーティングシステム機能」604は、仮想配布環境100に関連するタスクを安全に取り扱う。SPU500は、「権利および監査オ

ペレーティングシステム機能」402のセキュリティ機能の多くを提供あるいはサポートする。「他のオペレーティングシステム機能」606は、一般的な機器機能を取り扱う。オペレーティングシステム全体602は、始めから「権利および監査オペレーティングシステム機能」604プラス「他のオペレーティングシステム機能」606を含むように設計されても、「権利および監査オペレーティングシステム機能」が「他のオペレーティングシステム機能」を提供する既存のオペレーティングシステムに付加されてもよい。

本実施例における「権利オペレーティングシステム」602は、多くの異なるタイプの機器600と共に作動し得る。例えば、権利オペレーティングシステムは、大型のメインフレームコンピュータ、「ミニコンピュータ」、およびパーソナルコンピュータおよび携帯用計算機器などの「マイクロコンピュータ」と共に作動し得る。また、権利オペレーティングシステムは、テレビジョンセットの上部のコントロールボックス、小型の携帯用「ページャ」、デスクトップラジオ、ステレオサウンドシステム、電話、電話スイッチ、または他のいずれもの電子機器中でも作動し得る。小型機器のみではなく大型機器上でも動作するこの能力は、「規模変更可能性(scalable)」と称される。「規模変更可能」オペレーティングシステム602とは、非常に様々なタスクを行う多くの異なる機器を通る基準化されたインタフェースがあり得ることを意味している。

「権利オペレーティングシステム機能」604は、本実施例において「サービスベース」である。例えば、「権利オペレーティングシステム機能」604は、より詳細な「サブ要求」を常に行うのではなく、または概要要求を満たすことに伴う基礎にある複雑さと関連させることをアプリケーションに要求するのではなく、アプリケーション608からの概要要求を取り扱う。例えば、アプリケーション608は、指定された情報を読み出すようにただ単に要求するだけでよい。すると、「権利オペレーティングシステム機能」604は、所望の情報がVDE保護コンテンツであるか否かを決定し、そうである場合は、情報を利用可能にするために必要となるプロセスを行い得る。この特徴は、「トランスペアレンシ(transparency)」と称される。「トランスペアレンシ」によって、アプリケーション608のためにタスクが容易になる。「権利オペレーティングシステム機能」604は、仮想

配布環境100について何も知らないアプリケーション608をサポートし得る。仮想配布環境100を「認識している」アプリケーション608は、仮想配布環境100のより詳細な利用を行い得る。

本実施例において、「権利オペレーティングシステム機能」604は「イベント駆動」される。「権利オペレーティングシステム機能」604は、条件が生じるか否かを決定するために電子機器600の状態を繰り返し検討するのではなく、機器600内の「イベント」あるいは「出来事」に直接応答し得る。

本実施例において、「権利オペレーティングシステム機能」604によって行われるサービスには、オペレーティングシステム602に配送される付加的な「コンポーネント」に基づいて拡張され得るものがある。「権利オペレーティングシステム機能」604は、異なる時点に異なる参加者によって送られる「コンポーネント」を集め、使用することができる。「コンポーネント」はオペレーティングシステム602を「規模変更可能」にする補助を行う。コンポーネントには、サービスが大型機器（例えば、マルチユーザ）上でどのように動作するかに対する小型機器上でどのように動作するかを変えることができるものもある。他のコンポーネントは、特定のアプリケーションあるいはアプリケーションのクラス（例えば、いくつかのタイプの計量およびいくつかのタイプの予算作成）と共に動作するように設計される。

電子機器600

好ましい実施の形態によって提供される電子機器600は、例えば、１つ以上のマイクロプロセッサおよび／またはマイクロコントローラおよび／または論理および／または数学計算を行う他の装置を含む電子装置のいずれもであり得る。これは、コンピュータ、コンピュータ端末、コンピュータと共に用いるための装置コントローラ、コンピュータと共に用いるための周辺機器、ディジタル表示装置、テレビ、映像および音声／映像投影システム、放送および／またはケーブル伝送と共に用いるためのチャネルセレクタおよび／またはデコーダ、遠隔制御装置、ビデオおよび／または音声レコーダ、コンパクトディスクプレーヤ、ビデオディスクプレーヤ、およびテーププレーヤを含むメディアプレーヤ、音声および／映

像増幅器、バーチャルリアリティ機械、電子ゲームプレーヤ、マルチメディアプレーヤ、ラジオ、電話、ビデオ電話、ファックス、ロボット、機械ツールなどを含む定格制御機械、および１つ以上のマイクロコンピュータおよび／マイクロコントローラおよび／または未だ存在していないものを含む他のCPUを含む他の装置であり得る。

図８は、電子機器600の一例を示す。電子機器600のこの例は、システムバス653を含む。この例において、１つ以上の従来の汎用中央処理装置（「CPU」）654がバス653に接続されている。バス653は、CPU654をRAM656、ROM658およびI/Oコントローラ660に接続する。１つ以上のSPU500もまた、システムバス653に接続され得る。システムバス653は、SPU500がCPU654と通信するのを許可し、また、CPUおよびSPUの両方がRAM656、ROM658およびI/Oコントローラ660と通信すること（例えば、共有されたアドレスおよびデータラインを通って）を可能にし得る。電源659は、SPU500、CPU654および図示されている他のシステムコンポーネントに電力を供給し得る。

図示されている例において、I/Oコントローラ660は第２の記憶装置652、キーボード／ディスプレイ612、614、通信コントローラ666およびバックアップ記憶装置668と接続される。バックアップ記憶装置668は、例えば、テープ670、フロッピィディスク、着脱可能なメモリカードなどのマスメディア上に情報を格納し得る。通信コントローラ666によって、ネットワーク672あるいは他の遠隔通信リンクを介して電子機器が他の電子機器と通信することが可能になり得る。異なる電子機器600は、異なるCPUおよびROS602の異なる例を用いても、互換性のある通信プロトコルおよび／またはセキュリティメソッドを代表的に用いる限り、相互動作し得る。この例において、I/Oコントローラ660は、CPU654およびSPU500が第２の記憶装置662、キーボード／ディスプレイ612、614、通信コントローラ666およびバックアップ記憶装置668からの読み出しおよび書込みを行うことを許可する。

第２の記憶装置662は、一般的な第２の記憶装置機能のために電子機器600が用いる同一の１つ以上の非安全な（non-secure）第２の記憶装置（一例として磁気ディスクおよびCD－ROMドライブ）を備えてもよい。いくつかの実施態様におい

ては、第２の記憶装置652の一部あるいは全体が、安全なエンクロージャに物理的に封入されている第２の記憶装置を備えていてもよい。しかし、多くの実施態様において第２の記憶装置を物理的に安全化することは実用的でもコスト有効的でもあり得ないので、第２の記憶装置652は、情報を第２の記憶装置652中に格納する前に情報を暗号化することによって安全に情報を格納するために用いられ得る。情報が格納される前に暗号化される場合、第２の記憶装置652への物理的アクセスあるいはそのコンテンツが、情報を容易にさらしたり、傷つけることはない。

この例における第２の記憶装置は、CPU654および／またはSPU500によって使用されるコードおよびデータを、電子機器600全体の動作を制御するために格納する。例えば、図８は、図７に示される「権利オペレーティングシステム」（「ROS」）602（VDE機能を提供するROSの一部604および他のOS機能を提供する部分606を含む）が第２の記憶装置652上に格納され得ることを示している。第２の記憶装置652はまた、１つ以上のVDEオブジェクト300を格納し得る。また、図８は、図７に示される安全なファイル610が、「安全なデータベース」あるいは管理ファイルシステム610の形態で第２の記憶装置652に格納され得ることを示している。この安全なデータベース610は、ROS602によって使用される情報を格納および組織化することによってVDE機能604を行い得る。従って、VDEおよび他のOS機能604および606を行うために実行されるコードおよびこれらの機能に関連づけられる安全なファイル610（VDEオブジェクト300も同様に）、第２の記憶装置652に格納され得る。第２の記憶装置652はまた、例えば、タスク管理、非VDEファイルなどのための他のオペレーティングシステム機能606によって使用される情報などの「他の情報」673も格納し得る。第２の記憶装置652中に示されているエレメントの部分は、これらのエレメントが変更を必要としないかぎり（ROM658が置き換えられた時を除いて）ROM658に格納され得る。特にROS602の部分は、望ましくはROM658（例えば、電力が与えられたときに電子機器600のための動作環境を確立する際に使用するための「ブートストラップ」ルーチン、POSTルーチン、など）中に含まれ得る。

図８は、第２の記憶装置652が、図７に示されるユーザアプリケーション608を

提供するコード（「アプリケーションプログラム」）を格納するためにも用いられ得ることを示している。図８は、２つの一般的なタイプのアプリケーションプログラム608、すなわち、「VDE認識」アプリケーション608aおよび非VDE認識アプリケーション608b、があり得ることを示している。VDE認識アプリケーション608aは、アクセスを行い、かつ、VDE機能604を詳細に利用するために、特にVDE100を考慮して少なくとも一部が設計され得る。ROS602が「トランスペアレンシ」の特徴を有しているために、非VDE認識アプリケーション608b（例えば、VDE100に特定的に設計されないアプリケーション）はまた、アクセスおよびVDE機能604を利用することもできる。

安全な処理ユニット500

好ましい実施の形態における各VDEノードあるいは他の電子機器600は、１つ以上のSPU500を含み得る。SPU500は、VDE100についてのすべての安全な処理を行うために用いられ得る。例えば、SPU500は、VDE保護オブジェクト300を復号化（あるいは非安全化）するために用いられる。また、SPU500は、暗号化および／または安全化された通信を（情報の認証および／またはエラー訂正有効性検査を用いることなどによって）管理するために用いられ得る。SPU500はまた、（銀行アカウントおよび／またはVDEノードトークン貯金アカウントからの前払い、クレジット、リアルタイム電子借方を介する）VDEオブジェクト300の使用管理、監査、また適切な場合は、支払いを含む安全なデータ管理プロセスも行い得る。SPU500は、そのようなVDEオブジェクト300に関連する他の取引も行い得る。

SPU物理的パッケージングおよびセキュリティバリア502

図６に示されるように、好ましい実施の形態において、SPU500は、機密および／または商業的に価値のある情報が安全に処理、暗号化および／または復号化され得る安全な処理環境を提供するための単一の集積回路「チップ」505として実装され得る。ICチップ505は、例えば、親指の爪程度のサイズの小型の半導体「ダイ」を備え得る。この半導体ダイは、半導体および金属導電性経路を含み得る。これらの経路は回路、従って、SPU500の機能性を規定する。これらの経路には、チップ505の外側「ピン」504に電気的に接続されるものがある。

図６および図９に示されるように、SPU500は、不正改変不可能なハードウェアセキュリティバリア502によって取り囲まれ得る。このセキュリティバリア502の一部は、SPU「ダイ」が入れられているプラスチックあるいは他のパッケージによって形成されている。SPU500内で生じる処理およびSPU500によって格納される情報は、外界から容易にアクセス可能ではないので、これらは非許可アクセスおよび不正改変から比較的安全である。すべての信号は、SPU500内の内部コンポーネントへの外界のアクセスを制限するBIU530によって提供される安全な制御された経路を介してバリア502を通過する。この安全な制御された経路は、SPU500内の秘密の情報およびリソースにアクセスする外界からの試みを妨げようとする。

ICチップのプラスチックパッケージを除去し、「ダイ」へのアクセスを達成することが可能である。また、（例えば、回路を動作させ、酸エッチングあるいは半導体層を除去して他の層を露出させる他の技術を用い、電子顕微鏡を用いてダイを観察および写真撮影するのと同時に、ダイ上の信号を収集および分析するために様々なタイプの論理アナライザおよびマイクロプローブを用いて）「ダイ」自体を分析および「リバースエンジニアリング」することも可能である。そのような攻撃を全く受けないシステムあるいは回路はないが、SPUバリア502は、攻撃を成功させるためには非常にコストがかかり、時間を消費する付加的なハードウェア保護も含み得る。例えば、イオン注入および／または他の制御技術がSPUダイ導電性経路を視覚的に認識することを非常に困難にし、SPU内部回路は空気および／または光にさらされると「自己有意破壊」するように製造され得る。SPU500は、電力を失うとコンテンツを失う内部メモリ中に秘密情報を格納し得る。回路は、マイクロプローブあるいは他の不正改変を検出し、不正改変が検出されると自己有意破壊する（あるいはSPUの他の部分を破壊する）SPU500に組み込まれ得る。これらおよび他のハードウェアベースの物理的セキュリティ技術は、不正改変不可能なハードウェアセキュリティバリア502に寄与する。

セキュリティバリア502のセキュリティをさらに増すために、例えば、以下のような１つ以上の物理的エンクロージャにSPU500を入れる、あるいは含ませることが可能である。エポキシあるいは他の「埋込み用樹脂」、付加的な自己有意破

壊、自己使用不可能（self-disabling）あるいは不正改変が検出されると活性化される他の特徴を含む別のモジュールエンクロージャ、パスワードあるいは動作のための他の認証の要求などの付加的なセキュリティ保護を提供する別のモジュールなどである。さらに、金属の別の層がダイに付加されることによって、酸エッチング、マイクロプロービングなどが複雑になり得る。メモリを「ゼロ化」するように設計された回路は、自己有意破壊の局面として含まれ得る。プラスチックパッケージ自体は、化学的および物理的「攻撃」に抵抗するように設計され得る。SPU500の内部のメモリは、ビットの位置を「シャッフル」し、それによってメモリ位置の値を電気的に決定する、特殊化されたアドレス指定およびリフレッシュ回路を有し得る。これらのおよび他の技術は、バリア502のセキュリティに寄与し得る。

いくつかの電子機器600において、SPU500は、装置マイクロコントローラまたは等価物、あるいは装置I/Oあるいは通信マイクロコントローラと共に、共通チップ（またはチップセット）505に集積化され得る。例えば、一つの好ましい実施の形態において、SPU500は、１つ以上の他のCPU（例えば、電子機器のCPU654）と単一のコンポーネントあるいはパッケージ中に集積化され得る。他のCPU654は、例えば、マイクロプロセッサ、他のマイクロコントローラ、および／またはアレイあるいは他の並列プロセッサなどのいずれもの中心制御論理構成であり得る。この集積化された構成によって、コスト全体が低下し、サイズ全体が小さくなり、SPU500とCPU654との間のより速い潜在的な相互作用が行われ得る。また、集積化されたSPU／CPUコンポーネントが広範に配布されたマイクロプロセッサラインの標準的な特徴である場合は、集積化によって、より広い配布が行われ得る。電子機器600のメインCPU654へ（あるいは、他の機器、または機器周辺マイクロコンピュータ、あるいは他のマイクロコントローラへ）のSPU500の組み込みによって、VDE100を実施する通常経費コストを実質的に低減し得る。集積化の際に考慮されるべきことには、実施コスト、製作コスト、所望の程度のセキュリティ、および小ささが含まれ得る。

SPU500は、CPU以外の装置とも集積化され得る。例えば、ビデオおよびマルチメディアアプリケーションについて、性能および／またはセキュリティ利点（全

体の設計に依存する）には、SPU500をビデオコントローラあるいはチップセットに集積化することから得られ得るものもある。SPU500はまた、ネットワーク通信チップあるいはチップセットなどに直接集積化され得る。高速通信アプリケーションにおけるある性能は、SPU500をモデムチップあるいはチップセットと集積化することからも得られ得る。これによって、スタンドアローンファックス機械などの通信機器へのSPU500の組み込みを促進し得る。SPU500は、CD-ROM装置、セットトップケーブル装置、ゲーム装置、および配布された情報を使用する、その情報へのアクセスを可能にする、その情報に関連する取引を行う、または配布された情報を消費する、様々な他の電子機器に集積化され得る。

SPU500内部アーキテクチャ

図9は、SPU500の一例の内部構造の詳細な図である。この例におけるSPU500は、単一のマイクロプロセッサ520と、ROM532およびRAM534として構成された、制限された量のメモリとを含む。より詳細には、SPU500のこの例は、マイクロプロセッサ520と、暗号化／復号化エンジン522と、DMAコントローラ526と、リアルタイムクロック528と、バスインタフェースユニット（「BIU」）530と、読み出し専用メモリ（ROM）532と、ランダムアクセスメモリ（RAM）534と、メモリ管理ユニット（「MMU」）540とを備えている。DMAコントローラ526およびMMU540は選択的であるが、これらがないとSPU500の性能に悪影響が与えられ得る。SPU500は、選択的なパターンマッチングエンジン524と、選択的な乱数ジェネレータ542と、選択的な算術アクセレータ回路544と、選択的な圧縮／圧縮解除回路546とを備え得る。共有されたアドレス／データバス構成536は、マイクロプロセッサ520および／またはDMAコントローラ526の制御下でこれらの様々なコンポーネント間で情報を移動させ得る。付加的なあるいは代替的な専用経路538は、マイクロプロセッサ520を他のコンポーネント（例えば、ライン538aを介して暗号化／復号化エンジン522に、ライン538bを介してリアルタイムクロック528に、ライン538cを介してバスインタフェースユニット530へ、およびライン538dを介してDMAコントローラへ、ライン538eを介してメモリ管理ユニット（MMU）540へ）接続し得る。

以下の章では、これらのSPUコンポーネントを各々詳細に検討する。

マイクロプロセッサ520

マイクロプロセッサ520は、SPU500の「プレーン」である。この例において、マイクロプロセッサは、ROM532および／またはRAM534内に（少なくとも一時的に）格納されたコードによって指定される一連のステップを実行する。好ましい実施形態におけるマイクロプロセッサ520は、ROM532および／または他のメモリに格納されている命令を実行するための専用中央処理構成（例えば、RISCおよび／またはCISCプロセッサユニット、マイクロコントローラ、および／または他の中央処理手段、あるいは望ましさの程度は低くなるが、大半のアプリケーションにおいて、プロセス特定専用制御論理）を備える。マイクロプロセッサ520は、回路設計（layout）の別々のエレメントであっても、安全なSPU500内の別々のパッケージであってもよい。

好ましい実施の形態において、マイクロプロセッサ520は、通常、電子機器600の動作の最もセキュリティに影響を受けやすい面を取り扱う。例えば、マイクロプロセッサ520は、VDE復号化、暗号化、あるコンテンツおよび／または機器使用制御情報、VDE安全化されたコンテンツの使用の記録、および他のVDE使用規則関連機能を管理し得る。

各SPU500および／または電子機器の第２のメモリ652に格納されているのは、例えば、ROS602ソフトウェア、アプリケーションプログラム608、VDE制御されたプロパティコンテンツおよび関連する情報を含むオブジェクト300、およびオブジェクトに関連づけられた情報およびVDE制御情報の両方を格納する管理データベース610の一例であり得る。ROS602は、一部には、VDEに関するオブジェクト300の使用を電子機器600によって制御するためのSPUマイクロプロセッサ520によって実行されることを意図されたソフトウェアを含む。以下で説明されるように、これらのSPUプログラムは、基本的な制御機能を行うための「ロードモジュール」を含む。これらの様々なプログラムおよび関連づけられたデータは、主にマイクロプロセッサ520によって実行および加工される。

リアルタイムクロック（RTC）528

好ましい実施の形態において、SPU500は、SPUのための信頼性のある不正改変

不可能な時間ベースとなるリアルタイムクロック回路（「RTC」）528を含んでいる。RTC528は、好ましい実施の形態において一日の時間および日付け（例えば、月、日および年）を記録し、従って、カレンダとクロックとの組み合わせを有し得る。信頼性のある時間ベースは、時間ベースの時間計量メソッド、「時間的に古い復号化鍵」および他の時間ベースSPU機能を実行するために重要である。

RTC528は、動作のために電力を受け取らなければならない。最適には、RTC528電源は、SPU500内に位置する小型バッテリあるいは他の安全なエンクロージャを備え得る。しかし、RTC528は、SPU500の外部にある外部に位置するバッテリなどの電源を用い得る。このような外部に位置するバッテリは、比較的途切れのない電力をRTC528を提供し、またSPU500内の揮発性RAM534の少なくとも一部を非揮発性に維持する。

一つの実施態様において、電子機器電源659は、SPU500に電力を与えるためにも用いられる。RTC528のための唯一の電源としていずれもの外部電源を用いることによって、少なくとも、SPU500が、外部電力の供給のいずれもの中断（あるいは重要な中断のいずれか）を認識し、そのような中断を記録し、VDEプロセスの一部あるいはすべてを行うSPU500の能力を不能にするなど、適切であり得るように応答しない限り、時間ベースのセキュリティ技術の有用性を大幅に低減させる。電力の中断は、例えば、電力不良によって活性化される回路を用いることによって達成され得る。電力不良感知回路は、１つ以上の電力不良イベントを記録するための関連づけられた論理を含む別の回路に電力を与え得る。キャパシタ放電回路は、この論理を動作させるために必要な一時的な電力を供給し得る。さらにまたはあるいは、SPU500は、RTC528の出力を、利用可能である場合は、ホスト電子機器600のクロック出力と時折比較し得る。相違が検出された場合には、SPU500は適切に応答し得、その応答は、相違の記録および／または少なくともいくつかの状況下でSPU500によって行われるプロセスの少なくとも一部を使用不能にすることを含む。

電力不良および／またはRTC528相違および／または他のイベントが、不正改変の可能性を示す場合、SPU500は、実行に関連する情報および／または暗号化鍵に関連する情報などの、SPUが格納する影響を受けやすい情報の一つ以上の部分を

自動的に破壊するか、特権化された介入なしにアクセス不可能にし得る。さらなるSPU動作を提供するために、適切であるように、VDE情報交換所、管理者および／または配布者が破壊された情報に代わらなければならない。これは、更新および／または置換データおよび／またはコードを遠隔的にダウンロードすることによって達成され得る。上記のようにプロセスおよび／または情報が不能にされるおよび／または破壊される場合、電子機器600は、RTC528を再初期化するために、適切なように管理者、情報交換所および／または配布者との安全なVDE通信を必要とし得る。それまでは安全なSPU500プロセスの一部あるいは全てが動作し得ない。

RTC528を設定および／または同期化するためのメカニズムを提供することが望ましくあり得る。好ましい実施の形態において、VDE電子機器600と別のVDE機器との間で通信が生じると、RTC528の出力は、「上位（senior）」であることが承認され制御を行うパーティの制御下で、制御されたRTC528出力時間と比較され得る。相違の場合は、通信において「下位（junior）」によって制御される参加者のRTC528をリセットすることを含む、適切な行動がとられ得る。

SPU暗号化／復号化エンジン522

好ましい実施形態において、SPU暗号化／復号化エンジン522は、データを迅速かつ効率よく暗号化および/または復号化するための特定目的ハードウェア（例えば、ハードウェア状態マシン（state machine））を提供する。ある実施態様においては、暗号化/復号化機能は、ソフトウェアの制御下でマイクロプロセッサ520によって代わりに行われ得るが、一般的に、特定目的暗号化/復号化ハードウェアエンジン522を設けると性能があがる。所望であれば、例えば１つ以上の回路素子を最適に共用するために、マイクロプロセッサ520は、同じ回路レイアウトに共に統合しうるプロセッサ回路部および専用暗号化/復号化論理の組合せを含み得る。

一般的に、SPU500によって扱われる大抵のデータおよびオブジェクトを保護するためには、計算上効率的かつ非常に安全な「バルク（bulk）」暗号化/復号化技術を使用することが好ましい。通信チャネルを確立し、いかなる転送されたパーミ

ッション、メソッド、および管理情報も安全化する電子機器600のアイデンティティを認証するための局面として、非常に安全な暗号化/復号化技術を使用することが好ましい。好ましい実施形態において、暗号化/復号化エンジン522は、対称鍵暗号化/復号化回路（例えば、DES、Skipjack/Clipper、IDEA、RC-2、RC-4など）および反対称（非対称）または公開鍵（「PK」）暗号化/復号化回路の両方を含む。公開/秘密鍵暗号化/復号化回路は、SPU500と、VDE管理者または他の電子機器600との間、つまりVDE安全サブシステム間の安全な通信の局面として主に使用される。対称的な暗号化/復号化回路は、SPU500が内在する電子機器600の補助記憶装置662に格納される大抵のデータを、「バルク」暗号化および復号化するために使用され得る。対称鍵暗号化/復号化回路はまた、VDEオブジェクト300内に格納されているコンテンツを暗号化および復号化するためにも使用され得る。

DESまたは公開/秘密鍵メソッドは、全ての暗号化機能に使用され得る。代替の実施形態においては、種々の暗号化に関連した機能に、DESおよび公開/秘密鍵メソッド以外の暗号化および復号化メソッドを使用し得る。例えば、同じ鍵を暗号化および復号化に使用する他のタイプの対称暗号化/復号化技術を、DES暗号化および復号化の代わりに使用することができる。好ましい実施形態は、暗号化/復号化エンジン522内の多数の専用回路、および/またはSPU500内の処理配置部（processing arrangement）を用いて複数の暗号化/復号化技術をサポートすることができる。

パターンマッチングエンジン524

任意のパターンマッチングエンジン524によって、パターンマッチング機能を行う特定目的ハードウェアを得ることができる。SPU500の行いうる機能の1つに、VDEオブジェクト300および他のアイテムを有効性検査/認証することが挙げられる。有効性検査/認証ではよく、特定の手法で同じかどうかを決めるために、長いデータストリングを比較する。さらに、（アクセスされたエレメントの論理的および/または物理的な（連続した）関係などの）特定の使用形式においては、特定のビットパターンに対してもしかしてあるかもしれない長いデータストリング（potentially long strings of data）、または他の重要なパターンに関連した測定

基準（metric）のサーチを必要としうる。パターンマッチングは、ソフトウェアの制御下でSPUマイクロプロセッサ520によって行うことができるが、特定目的ハードウェアパターンマッチングエンジン524を設けることによって、パターンマッチング処理の速度をあげ得る。

圧縮/圧縮解除エンジン546

VDEオブジェクト300に格納された、またはそこから放出されたコンテンツを、例えば圧縮および/または圧縮解除するために、SPU500内に任意の圧縮/圧縮解除エンジン546を設置し得る。圧縮/圧縮解除エンジン546は、ハードウェア回路部を用いて1つ以上の圧縮アルゴリズムを実施し、圧縮/圧縮解除動作のパフォーマンス（これは、さもなくばマイクロプロセッサ520、またはSPU500の外部で動作しているソフトウェアによって行われる）を改善し得る。通常配布前に圧縮され、その圧縮解除速度が重要である映像または音声などのデータの放出において、圧縮解除が重要となる。場合によって、使用をモニタリングする目的に有用な情報（レコード分離部または他のデリミッタなど）は圧縮層の下に「隠れて」おり、この層は、この情報が検出されSPU500内で使用される前に削除しなければならない。

乱数発生器542

任意の乱数発生器542は、（例えば、量子雑音のような本質的に予期し得ない物理的過程から）無作為な値を発生するために、専用のハードウェア回路部を提供し得る。そのような無作為な値は、特に、暗号化鍵または固有の識別子を構成するのに、また疑似ランダム列の発生を初期化するのに有用である。乱数発生器542は、使用あたり単一ビットほどの小さい値も含めて、いかなる都合の良い長さの値も発生し得る。乱数発生器542によって発生された値を連鎖（concatenating）させることによって、任意の大きさの乱数を構成し得る。乱数発生器542によって発生される無作為鍵およびシードと、SPU500内の暗号化/復号化エンジン522または暗号技術的アルゴリズムによる繰り返しの暗号化とから暗号技術上強力な疑似ランダム列を発生し得る。このような列は例えば秘密ヘッダに使用されて、暗号化分析によって暗号鍵を判定しようとする試みをくじくことができる。

演算アクセレレータ５４４

大きい数値を伴った乗算およびべき乗などの数学的な計算を迅速に行いうるハードウェア回路部の形態で、任意の演算アクセレレータ５４４をSPU５００内に設置しうる。特定の非対称的暗号化/復号化演算に必要となる計算を援助するために、これらの計算は、例えば、マイクロプロセッサ５２０または暗号化/復号化エンジン５２２によってリクエストされ得る。そのような演算アクセレレータは、当業者によく知られている。実施態様によっては、独立した演算アクセレレータ５４４は省略され、いかなる必要となる計算もソフトウェアの制御下でマイクロプロセッサ５２０によって行われ得る。

DMAコントローラ５２６

DMAコントローラ５２６は、マイクロプロセッサ５２０に各個別のデータ転送を処理させる必要なしに、アドレス/データバス５３６への情報転送を制御する。典型的には、マイクロプロセッサ５２０は、転送すべきターゲット、行き先アドレスおよびバイト数をDMAコントローラ５２６に書き込み、次いでDMAコントローラ５２６は、SPU５００のコンポーネント間（例えば、ROM５３２からRAM５３４へ、暗号化/復号化エンジン５２２とRAM５３４との間、バスインターフェースユニット５３０とRAM５３４との間など）にデータブロックを自動的に転送し得る。DMAコントローラ５２６は、多数の転送を同時に扱うために多数のチャネルを有し得る。いくつかの実施態様において、独立のDMAコントローラ５２６は省略することができ、いかなる必要なデータ移動も、ソフトウェアの制御下でマイクロプロセッサ５２０によって行われ得る。

バスインターフェースユニット（BIU）５３０

バスインターフェースユニット（BIU）５３０は、SPU５００と、安全性バリア５０２を越えた外界との間で情報を通信する。適切なドライバソフトを加えた図９に示されるBIU５３０は、図６に示される「機器リンク（appliance link）」５１０を含み得る。好ましい実施形態において、バスインターフェースユニット５３０は、USARTまたはPCIバスインターフェースにならってモデル化（modelled）され得る。本例においては、BIU５３０は、図８に示される電子機器システムバス６５３にSPU５００を接続する。BIU５３０は、SPU５００内の内部コンポーネントおよびそれらのコンテンツへの承認さ

れていないアクセスを防ぐように設計される。これは、SPU500に関連する信号をマイクロプロセッサ520上でランされる制御プログラムによって処理することだけを許可し、SPU500の内部エレメントへの直接アクセスをサポートしないことによって実施される。

メモリ管理ユニット540

メモリ管理ユニット(MMU)540は、存在すれば、メモリ管理および仮想メモリ管理機能のためのハードウェアサポートを提供する。また、安全な実行空間のハードウエアコンパートメント化(hardware compartmentalization)を強化する(例えば、比較的低信頼なタスクが、より高信頼なタスクを改変することを防ぐ)ことにより、向上した安全性も提供し得る。SPU500によってサポートされる安全処理環境(「SPE」)503のアーキテクチャの論議に関連して、以下により詳細に説明する。

MMU540は、また、例えばアドレスマッピングなど、メモリ管理に関連したハードウェアレベルのサポート機能も提供し得る。

SPUメモリアーキテクチャ

好ましい実施形態において、SPU500は、３種類の汎用メモリを使用する：

（１）内部ROM532；

（２）内部RAM534；および

（３）外部メモリ(典型的には、ホスト電子機器によって供給されるRAMおよび/またはディスク)

SPU500内の内部ROM532およびRAM534は、安全動作環境および実行空間を提供する。コスト制限、チップ加工サイズ、複雑性および他の制限から、SPUが安全に処理するために必要となる情報を全て格納するために十分なメモリをSPU500内に設置できないかもしれない。SPU500内に含まれ得るROM532およびRAM534の容量には実際的な限界があるため、SPU500は、外部メモリに情報を格納し、必要に応じて、この情報を移動させて安全内部メモリ空間へ出し入れし得る。この場合、SPUによって行われる安全処理ステップは、典型的に、制限のある利用可能な内部メモリ空間に「ページイン」、およびそこから「ページアウト」し得る、小さく安全

にパッケージングされたエレメントに分割されなければならない。SPU500の外部にあるメモリは安全でないかもしれない。外部メモリは安全でないかもしれないため、SPU500は、コードおよび他の情報を、外部メモリに格納する前に暗号化し、かつ暗号技術的にシールし得る。同様に、SPU500は、典型的には、外部メモリから得た暗号化形式のコードおよび他の情報を、それに基づく処理（例えば実行）前に復号化しなければならない。好ましい実施形態において、SPU500内の潜在的なメモリ制限に取り組むために使用される一般的なアプローチが２つある。第１の場合、小さい、安全にパッケージングされたエレメントは、安全データベース610に含まれる情報を表す。第２の場合、そのようなエレメントは、保護された（例えば、暗号化された）仮想メモリページを表し得る。仮想メモリページは、安全データベース610に格納された情報エレメントと対応し得るが、これは本例のSPUメモリアーキテクチャにおいて必要でない。

以下に、これらの３つのSPUメモリリソースのそれぞれをより詳細に議論する。

SPU内部ROM

SPU500読み出し専用記憶素子（ROM）532、または匹敵する目的の（comparable purpose）装置は、特定のプログラムおよび他の情報の安全内部不揮発性記憶装置を提供する。例えば、ROM532は、SPU制御ファームウェア508などの「カーネル」プログラム、また所望であれば、暗号化鍵情報および特定の主要な「ロードモジュール」を格納し得る。「カーネル」プログラム、ロードモジュール情報、および暗号化鍵情報は、SPU500の特定の基本的な機能の制御を可能にする。装置の構成に少なくとも部分的に依存しているコンポーネント（例えば、POST、メモリアロケーション、およびディスパッチャ）は、特定のインストレーションまたはアプリケーションに必要であると判定された追加のロードモジュールと共に、ROM532にロードされ得る。

好ましい実施形態において、ROM532は、マスクされたROM532aと、EEPROMおよび/または等価の「フラッシュ」メモリ532bとの組合せを含み得る。EEPROMまたはフラッシュメモリ532bは、更新および/または初期化する必要のある、特定の暗

号化鍵などのアイテムを格納するために使用される。EEPROMおよび/またはフラッシュメモリ532bを設置することによるさらなる利点は、SPU500に永続的に格納されているいかなるロードモジュールおよびライブラリ機能も、特定サイトにおける代表的な用途に基づいて最適化できることである。これらのアイテムはまた、NVRAM534bにも格納され得るが、EEPROMおよび/またはフラッシュメモリ532bの方がコスト効率がより高い。

マスクされたROM532aは、フラッシュおよび/またはEEPROM532bよりコストが低くなり得、SPUソフトウェア/ファームウェアの永久部分(permanent portions)を格納するために使用され得る。そのような永久部分は、例えば、RTC528、暗号化/復号化エンジン522、割り込み処理ハンドラ(interrupt handlers)、鍵発生器などのハードウェア素子とインターフェースをとるコードを含み得る。SPU500によって提供されるいくつかのオペレーティングシステム、ライブラリコール、ライブラリ、および多くのコアサービスもまた、マスクされたROM532aに内蔵され得る。さらに、いくつかのより一般的に使用される実行可能物(executables)もまた、マスクされたROM532aに多分に内蔵され得る。更新の必要な、またはSPU500からパワーが解除された場合に消失する必要のあるアイテムは、マスクされたROM532aに格納されるべきではない。

状況によっては、RAM534aおよび/またはNVRAM534b(NVRAM534bは、例えば、コンスタントに電力が供給される従来のRAMである)は、ROM532の役割の少なくとも一部を実施し得る。

SPU内部RAM

SPU500汎用RAM534は、とりわけ、安全処理のための安全実行空間を提供する。好ましい実施形態において、RAM534は、高速RAM534aとNVRAM(「不揮発性RAM」)534bとの組合せのような異なるタイプのRAMを含む。RAM534aが揮発性を有し得る一方で、NVRAM534bは、好ましくはバッテリ支援されるか(backed)、さもなくば不揮発性である(すなわち、電源がオフにされた場合もその内容を失わない)ように

配置される。

高速RAM534aは、実行されるアクティブコード、および関連データストラクチ

ャを格納する。

NVRAM534bは、好ましくは、SPU500がVDE管理者と通信する初期化処理の一部として予めロードされた特定の鍵およびサマリ値(summary values)を含み、またSPU500の動作に関連した変換可能または変換している情報も格納し得る。安全性の理由のために、特定の非常に影響を受けやすい情報(例えば、内部発生秘密鍵などの特定のロードモジュールおよび特定の暗号鍵関連情報)は、SPU500にロード、またはSPU500によって内部発生される必要が時にあるが、いったんロードまたは内部発生されるとSPUから出てはならない。この好ましい実施形態においては、SPU500の不揮発性ランダムアクセスメモリ(NVRAM)534bが、そのような非常に影響を受けやすい情報を安全に格納するために使用され得る。NVRAM534bはまた、頻繁に変換し得るデータであるが、電源が落とされた際、または電源停止モードの際には消失してはならないデータを格納するためにもSPU500によって使用される。

NVRAM534bは、好ましくは、フラッシュメモリアレイであるが、それに加えてまたはその代わりに、十分な速度およびコスト効率を有する、電気的に消去可能なプログラム可能な読み取り専用メモリ(EEPROM)、スタティックRAM(SRAM)、バブルメモリ、３次元ホログラフィックまたは他の電気光学メモリなど、もしくは他の書き込み可能(例えば、ランダムアクセス可能な)不揮発性メモリであり得る。

SPU外部メモリ

SPU500は、SPUの外部にあるメモリ装置に特定の情報を格納できる。利用可能であれば、電子機器600のメモリはまた、SPU500ソフトウェアのいかなる装置外部部分もサポートするために使用され得る。SPU500に外部メモリを使用させることによって特定の利益が得られる。一例として、ホスト電子機器600内の、RAM656および/またはROM658の不揮発性部分などの不揮発性読み取り/書き込みメモリを使用することによって、SPU500の内部メモリのサイズを小さくし得る。

そのような外部メモリは、SPUプログラム、データおよび/または他の情報を格納するために使用され得る。例えば、VDE制御プログラムは、少なくともその一

部は、実行前に、メモリにロードされ、SPU500に通信され、その中において復号化される。そのような制御プログラムは、再び暗号化され、その後のSPU500による実行のために格納され得る外部メモリに通信されて戻される(communicated back)。「カーネル」プログラムおよび/もしくは一部または全ての非カーネル「ロードモジュール」が、SPU500によってその外部にあるメモリに格納され得る。安全データベース610は比較的大きくなり得るため、SPU500は、一部または全ての安全データベース610を外部メモリ内に格納し、必要に応じてSPU500に部分的にコールすることができる。

前述したように、SPU500の外部にあるメモリは安全でないかもしれない。従って、安全性が必要となる場合、SPU500は、外部メモリに書き込む前に安全情報を暗号化し、外部メモリから読み出した安全情報を使用前に復号化しなければならない。暗号化層はSPU500内に存在する安全化処理および情報(例えば、暗号化アルゴリズムおよび鍵)に依存するため、暗号化層はSPU安全バリア502を効果的に「拡張」して、SPU500の外部にあるメモリに格納された情報を保護する。

SPU500は、幅広い異なる種類の外部メモリを使用することができる。例えば、外部メモリは、ディスク；外部EEPROMまたはフラッシュメモリ658；および/または外部RAM656などの電子機器補助記憶装置652を含み得る。外部RAM656は、外部不揮発性(例えば、コンスタントに電圧が供給される)RAMおよび/またはキャッシュRAMを含み得る。

SPU500のローカルにある外部RAMを使用することによって、SPUの外部に格納された情報へのアクセス時間が有意に改善される。例えば、外部RAMは以下のことに使用され得る：

C　(有意な電源またはシステム故障中の、フラッシュまたはハードディスクへの転送を想定して)メモリイメージページおよびデータストラクチャを、それらをフラッシュメモリまたは外部ハードディスクへ格納する前にバッファリングすること；

C　VDEオブジェクト300から放出されたデータのための暗号化および復号化バッファを提供すること。

C　SPU500に安全仮想メモリ環境を設けるための局面として、その時点で使用さ

れている「スワップブロック(swap blocks)」およびVDEデータストラクチャをキャッシュ(cache)すること。

C　例えば、補助記憶装置652へのSPUによるアクセスの頻度を減少するために、および/または他の理由により、他の情報をキャッシュすること。

デュアルポート外部RAMは、SPUバスインターフェースユニット530およびSPUマイクロプロセッサ520のデータ移動オーバーヘッドを減少できるため、SPU500の性能を改善するために特に効果的であり得る。

実質的に全てのデータ構造へのアクセス時間を有意に改善するために、SPU500のローカルにある外部フラッシュメモリを使用することができる。最も利用可能なフラッシュ記憶装置は書き込み寿命に限界があるため、フラッシュ記憶装置は、フラッシュメモリの寿命期間の間に生じる書き込みの回数を考慮する必要がある。従って、頻繁に書き込みされる一時的なアイテムを一時的に格納すること(flash storage)は好ましくない。外部RAMが不揮発性である場合には、フラッシュ(またはハードディスク)への転送は必要でないかもしれない。

SPU500によって使用される外部メモリは、以下の２つのカテゴリを含み得る：

C　SPU500専用の外部メモリ、および

C　電子機器600と共用されるメモリ。

VDE実施態様によっては、電子機器600のCPU654または他の素子と、メモリ(例えば、電子機器RAM656、ROM658、および/または補助記憶装置652)を共用することは、VDE安全データベース管理ファイル610、およびSPU500の外部に格納される必要のある情報を格納するために最もコスト効果のある手法である。汎用ファイル格納のために使用されるホストシステムハードディスク補助メモリ652は、例えば、VDE管理ファイル610を格納するためにも使用され得る。SPU500は、外部メモリへの独占的なアクセス(例えば、BIU530によって提供されるローカルバス高速接続)を与えられ得る。専用および共用外部メモリの両方を設置することもあり得る。

＊＊＊＊＊＊

上では、電子機器600の一例のハードウェア構成を説明した。以下の節におい

ては、好ましい実施形態である「権利オペレーティングシステム」(「ROS」)602のストラクチャおよび動作を含む、好ましい実施形態によって提供される電子機器600のソフトウェアアーキテクチャの一例を説明する。

権利オペレーティングシステム602

好ましい実施形態における権利オペレーティングシステム(「ROS」)602は、コンパクト、安全、イベント駆動型、サービスベース、「コンポーネント」志向の分散型多処理オペレーティングシステム環境であり、VDE情報安全制御情報、コンポーネント、およびプロトコルと、従来のオペレーティングシステムの概念とを統合している。従来のオペレーティングシステムと同様、好ましい実施形態によって提供されるROS602は、コンピュータシステムのハードウェアリソースを管理し、通信装置を含むインプットおよび/またはアウトプット装置にまで管理機能の範囲を拡張するソフトウェアの一部である。また従来のオペレーティングシステムと同様に、好ましい実施形態ROS602は、特定のハードウェア実施態様間の差、およびそれらの多くの細部にわたる複雑性を隠すための基本機能と抽象層との首尾一貫したセットを提供する。多くのまたはほとんどのオペレーティングシステムにおいて見られるこれらの特性に加えて、ROS602は、安全VDE取引管理および他のオペレーティングシステムでは見られない他の有利な特徴を提供する。以下は、好ましい実施形態におけるROS602によって提供される有利な特徴の一部の部分的なリストである：

規格化されたインターフェースにより基本機能の首尾一貫したセットが提供される

C　プログラミングを単純化する

C　同じアプリケーションを多くの異なるプラットホーム上でランできる

イベント駆動型

C　機能分解(functional decomposition)を容易にする

C　拡張可能

C　状態遷移および/または処理志向イベントを適合させる

C　タスク管理を単純化する

Ｃ　内部処理通信を単純化する

サービスベース

Ｃ　単純かつトランスペアレントな規模変更性(scalability)を可能にする

Ｃ　マルチプロセッササポートを単純化する

Ｃ　マシーン依存性(machine dependencies)を隠蔽する

Ｃ　ネットワーク管理およびサポートを容易にする

コンポーネントベースアーキテクチャ

Ｃ　独立的に送達可能な安全コンポーネントに基づく処理

Ｃ　処理制御のコンポーネントモデルは、要件に基づいて再構成できる異なる一連のステップを許容することができる

Ｃ　コンポーネントは(許可を受けて)追加、削除、または改変され得る

Ｃ　予め定義されたおよびユーザ定義されたアプリケーションイベントにわたる完全な制御情報

Ｃ　独立した実行可能物でイベントを個別に制御できる

安全

Ｃ　安全通信

Ｃ　安全制御機能

Ｃ　安全仮想メモリ管理

Ｃ　曝されること(exposure)から保護された情報制御ストラクチャ

Ｃ　データエレメントは有効性が検査され、相互に関連され、およびアクセス制御される

Ｃ　コンポーネントは独立的に暗号化され、有効性検査される

Ｃ　コンポーネントは、エレメントの非承認的な使用を防ぐために強く相互関連される

Ｃ　制御ストラクチャおよび安全化された実行可能物を、不正改変に対する保護のために使用する前に有効性検査する

Ｃ　I/Oレベルで安全性に対する考慮を統合する

Ｃ　放出時に情報のオンザフライ復号化を提供する

Ｃ　安全商用取引ネットワークを可能にする

Ｃ　フレキシブルな鍵管理を特色とする

規模変更性

Ｃ　多くの異なるプラットホームに対して高い規模変更性を有する

Ｃ　マルチプロセッサ環境における同時処理をサポートする

Ｃ　多数の協同プロセッサをサポートする

Ｃ　いなかる数のホストまたは安全プロセッサもサポートする

Ｃ　制御構造およびカーネルは、リコンパイルすることなく、種々のホストプラットホーム、およびターゲットプラットホーム内の異なるプロセッサに容易に移植可能である

Ｃ　遠隔処理をサポートする

Ｃ　リモートプロシージャコール（Remote Procedure Calls）を内部ＯＳ通信に使用し得る

高統合性

Ｃ　追加のオペレーティングシステム層として、ホストプラットホームと共に高度に統合できる

Ｃ　従来ＯＳプラットホーム「の上にある」ＯＳ層を使用して、安全化されたコンポーネントおよび情報の非安全格納を許可する

Ｃ　取引管理およびコンテンツアクセスのための一般的用途パラダイムを提供するために、ホストオペレーティングシステムと共にシームレスに統合することができる

Ｃ　統合は多くの形態をとり得る：デスクトップのためのオペレーティングシステム層（例えば、DOS、Windows、Macintosh）；デバイスドライバおよびネットワークサービスのためのオペレーティングシステムインターフェース（例えば、UnixおよびNetware）；ならびに「ロウエンド」セットトップのための専用コンポーネントドライバは、多くの例の中の一部であり、従来およびリアルタイムオペレーティングシステムに統合され得る。

分散型

Ｃ　制御情報および相互制御情報の配布およびメカニズムを提供する

Ｃ　分散された、非同期配置にされたどのＶＤＥノードにおいても、制御された処理の条件付きの実行をサポートする

Ｃ　分散環境における制御された権利委譲

Ｃ　取り扱いおよび制御のチェーンをサポートする

Ｃ　分散され、時に接続され、それ以外においては非同期的にネットワーク化されたデータベースのための管理環境

Ｃ　リアルタイムおよび時間に無関係なデータ管理

Ｃ　「代理人（ａｇｅｎｔ）」処理をサポートする

トランスペアレント

Ｃ　既存のオペレーティングシステムにシームレスに統合され得る

Ｃ　その使用のために特に書かれたわけでないアプリケーションをサポートできる

ネットワークフレンドリ

Ｃ　内部ＯＳストラクチャは、処理を分散するためにＲＰＣを使用し得る

Ｃ　サブネットは、単一ノードとしてまたは独立的にシームレスに動作し得る

オペレーティングシステムに関する一般背景

「オペレーティングシステム」は、プログラマーがコンピュータシステムのためのアプリケーションをより簡単に作成することができるように、コンピュータシステムリソースを組織化するための制御メカニズムを提供する。オペレーティングシステムは、一般的に使用される機能を提供し、（例えば、異なる販売者によって製造され得る）異なるコンピュータハードウェアおよびアーキテクチャ間の互換性を確実にすることを助けることによってこれを行う。オペレーティングシステムは、また、コンピュータ「周辺機器」製造業者がより簡単に互換性のある装備をコンピュータ製造業者およびユーザに供給できるようにする。

コンピュータシステムは、通常いくつかの異なるハードウェアコンポーネントから作られる。これらのハードウェアコンポーネントは、例えば以下を含んでいる：

命令を実行するための中央処理ユニット（ＣＰＵ）；

実行命令、およびそれらの命令によって動作、またはそれらをパラメータ表示(parameterizing)するデータを格納するためのメインメモリセル(例えば、「RAM」または「ROM」)のアレイ；ならびに

メインメモリセルのイメージを格納するための名前付きエレメント(「ファイルシステム」)を反映するように組織化された１つ以上の補助記憶装置(例えば、ハードディスクドライブ、フロッピーディスクドライブ、CD-ROMドライブ、テープ読み取り器、カード読み取り器、または「フラッシュ」メモリ)。

ほとんどのコンピュータシステムはまた、キーボード、マウス、ビデオシステム、プリンタ、スキャナ、および通信装置などのインプット/アウトプット装置も含む。

CPUの実行能力を、利用可能なRAM、ROM、および補助記憶装置と組織化し、プログラマーにより使用される際に一般的に使用される機能を提供するために、「オペレーティングシステム」と称されるソフトウェアの１つが通常他のコンポーネントと共に含まれる。代表的には、この１つのソフトウェアは、電源がコンピュータシステムに入り、ハードウェアの診断が終了した後に実行を開始するように設計される。その後、CPU、メインメモリ、および補助メモリ装置の使用は全て、通常、この「オペレーティングシステム」ソフトウェアによって管理される。また、ほとんどのコンピュータオペレーティングシステムは、典型的に、これらの装置に伴う一般的に使用される機能を含めて、それらの管理機能をI/Oおよび他の周辺機器にまで範囲を拡張するためのメカニズムを含む。

オペレーティングシステムを通じてCPU、メモリ、および周辺機器を管理することによって、基本機能およびハードウェア細部を覆い隠すための抽象層の首尾一貫したセットによって、プログラマーは複雑なアプリケーションをより簡単に作成することができる。さらに、コンピュータのハードウェアリソースをオペレーティングシステムで管理することによって、異なる製造業者間の設計および装備要件の多くの差を隠すことができる。さらに、異なる製造業者の基本ハードウェアおよび周辺機器をかなり少ない作業でサポートすることができ、アプリケーションを同じオペレーティングシステムを有する他のユーザとより簡単に共用できる。

有意な利点を提供するオペレーティングシステムであるROS602

ROS602は「オペレーティングシステム」である。ROS602は、電子機器600のリソースを管理し、電子機器のためのアプリケーション608を書くプログラマーに、一般的に使用される機能のセットを提供する。好ましい実施形態における「ROS602」は、SPU500内のハードウェア（例えば、CPU、メモリ、安全RTC、および暗号化/復号化エンジン）を管理する。ROSはまた、電子機器600内の１つ以上の汎用プロセッサ内のハードウェア（例えば、CPUおよびメモリ）も管理し得る。ROS602は、電子機器に取り付けられた周辺装置などの他の電子機器ハードウェアリソースも管理する。例えば、図７を参照すると、ROS602は、キーボード612、ディスプレイ614、モデム618、ディスクドライブ620、プリンタ622、およびスキャナ624を管理し得る。ROS602はまた、安全なデータベース610、および安全なデータベース610を格納するために使用される記憶装置（例えば、「補助記憶装置」652）も管理し得る。

ROS602は、多数のプロセッサをサポートする。好ましい実施形態におけるROS602は、いくつもの局所および/または遠隔プロセッサをサポートする。サポートされるプロセッサは、少なくとも２つのタイプ（１つ以上の電子機器プロセッサ654、および/または１つ以上のSPU500）を含み得る。ホストプロセッサCPU654は、格納、データベース、および通信サービスを提供し得る。SPU500は、暗号技術的および安全化された処理実行サービスを提供し得る。ROS602によってサポートされる多様な制御および実行ストラクチャは、制御情報の処理が制御可能な実行スペース内で生じることを要件とし得る--この制御可能な実行スペースはSPU500によって提供され得る。追加のホストおよび/またはSPUプロセッサは、効率および/または能力を増加し得る。ROS602は、追加のプロセッサリソースおよび/または能力を提供するために、電子機器600の遠隔にあるさらなるプロセッサを、（例えば、ネットワーク、または他の通信リンクを通じて）アクセス、コーディネイトおよび/または管理し得る。

ROS602は、サービスベースである。好ましい実施形態において、ホストプロセッサ654および/または安全プロセッサ（SPU500）を使用して提供されるROSサービ

スは、「遠隔プロシージャコール」(「RPC」)内部処理リクエストストラクチャを使用してリンクされている。最小限に時間に依存し、ホストのネットワーク上の協同プロセッサに分散され得る内部処理サービスを、協同プロセッサは、RPCメカニズムを用いてリクエストし得る。ROS602によって提供されるマルチプロセッサアーキテクチャは、任意の数のホストまたは安全プロセッサをサポートするために、簡単に拡張することができる。この拡張性は、高いレベルの規模変更性をサポートする。また、サービスにより、機能は、異なる装備に異なって実行され得る。例えば、１人のユーザによる使用度が低い小型機器は、多くのユーザによる使用度の高い非常に大型な機器とはかなり異なる技術を使用したデータベースサービスを実行し得る。これは規模変更性の他の局面である。

ROS602は、分散処理環境を提供する。例えば、ユーザのリクエストを履行するために、情報および制御ストラクチャが、必要に応じて自動的、かつ安全にサイトの間を渡ることを可能にする。ROS602の分散処理特色の下にあるVDEノード間の通信は、前述したように内部処理サービスリクエストを含み得る。ROS602は、いかなるVDEノード内においても制御されたプロセッサの条件および/または状態に依存した実行をサポートする。処理が実行されるロケーションおよび使用される制御ストラクチャは、局所的に常駐し、遠隔アクセス可能であり、または遠隔システムでの実行をサポートする処理によって支援される。

ROS602は、例えば、「代理人」が遠隔環境において動作することを許可するために必要となる制御ストラクチャの配布を含む制御情報の配布を提供する。従って、ROS602は、「代理人」処理のために生じる要件の一部として、実行および/または情報制御を渡すための施設を提供する。

所望であれば、ROS602は、「リアルタイム」接続であり得るかもしれない非常に狭い帯域幅の接続にわたって、制御情報を独立的に配布し得る。好ましい実施形態により提供されるROS602は、「ネットワークフレンドリ」であり、どのレベルのネットワークプロトコルとも実行され得る。いくつかの例として、e-メール、およびISOモデルの「Layer 5」付近における直接接続が含まれる。

ROS602配布処理(および配布情報の関連監査)は、自らがそのような制御ストラ

クチャを用いる制御されたイベントである。この「反映型」配布処理メカニズムは、ROS602が、権利およびパーミッションを制御下で安全に配布し、情報コンテンツの使用特性を効果的に限定できるように許可する。分散環境での制御された権利委譲およびこのアプローチをサポートするためにROS602によって使用される安全処理技術は、有意な利点を提供する。

ROS602内の特定の制御メカニズムは「相互的」である。相互制御メカニズムは、同じまたは他のロケーションにおける１つ以上のコンポーネントと制御された状態で相互作用する１つ以上の制御コンポーネントを、１つ以上のロケーションに位置させる。例えば、ユーザのロケーションにおけるオブジェクトコンテンツに関連した使用制御は、使用制御の配布、使用制御の監査、および使用制御に伴うユーザリクエストを処理するための論理を統治する配布者のロケーションにおける相互制御を有し得る。ユーザのロケーションにおける使用制御は（１つ以上の使用の局面を制御することに加えて）、配布者のための監査、および配布者による処理のための使用制御に関連したフォーマットリクエストを用意し得る。相互制御の両エンドにおける処理は、さらに他の処理によって制御され得る（例えば、配布者は、使用制御メカニズムの製造数の予算によって限定され得る）。相互制御メカニズムは、多くのサイト、および多くのレベルにまで（例えば、作成者から配布者からユーザへと）拡張し得、いかなる関係（作成者/配布者、配布者/ユーザ、ユーザ/ユーザ、ユーザ/作成者、ユーザ/作成者/配布者など）も考慮し得る。相互制御メカニズムは、VDE100において、分散環境における関係およびアグリーメントを示すための使用が多い。

ROS602は規模変更可能である。ROS602制御ストラクチャおよびカーネルの大部分が、リコンパイルなしに種々のホストプラットホームに容易に移植可能である。許可機関がこの種の活性化を許可すれば、いかなる制御ストラクチャも配布（または再配布）され得る。ROS602内の実行可能なリファランスは、ターゲットプラットホームに移植可能である。ROS602の異なる実例では、リファランスを異なるリソースを用いて実行し得る。例えば、ROS602の１つの例においてはSPU500を使用してタスクを実行する一方で、ROS602の他の例においては、ソフトウェアにおいてSPUをエミュレートしている保護されたメモリにおいてランされるホスト

処

理環境を使用して同じタスクを実行し得る。ROS602制御情報は同様に移植可能である；多くの場合、イベント処理ストラクチャは、単一のコンピュータ内の協同プロセッサ間の場合と同じくらい簡単に、機械とホストプラットホームとの間を渡される。使用度が異なる機器、および/またはROS602機能が利用可能なリソースは、これらの機能を非常に異なった手法で実行し得る。十分なリソースがなければ、サービスによっては完全に省略され得る。他の箇所において説明したように、ROS602は、どのサービスが利用可能で、与えられたイベントに基づいてどのように続行すればよいのかを「知っている」。リソースが欠けていたり、不十分である場合、全てのイベントが処理可能ではないかもしれない。

ROS602はコンポーネントベースである。好ましい実施形態においてROS602によって提供される多くの機能性は、（例えば、適切に安全な状態および承認の下で）安全かつ独立的に送達可能、置換可能、および改変可能な「コンポーネント」に基づき得る。さらに、「コンポーネント」は自らが独立的に送達可能なエレメントから作られ得る。ROS602は、実行時に、（好ましい実施形態によって提供される「チャネル」と称される構造を用いて）これらのエレメントを共にアセンブルし得る。例えば、SPU500による実行のための「ロードモジュール」は、課金または計量（metering）などのタスクを行うために、１つ以上の「メソッドコア」、メソッドパラメータ、および、ROS602が共にコレクトしアセンブルし得る他の関連データストラクチャを参照し得る。異なるユーザは、異なる組合せのエレメントを有し得、いくつかのエレメントは、適切な認証を受けたユーザによってカスタマイズ可能であり得る。これにより、フレキシビリティが上がり、エレメントが再利用されることが可能になり、他の利点も生じる。

ROS602は、非常に安全である。ROS602は、情報制御構成をエンドユーザまたはコンジットホスト（conduit host）によって曝されることから保護するメカニズムを提供する。ROS602は、情報、VDE制御ストラクチャ、および制御実行可能なものを強力な暗号化および有効性検査メカニズムを用いることにより保護することができる。これらの暗号化および有効性検査メカニズムは、検知されない不正改

変に対して高い防御を有するように設計される。ROS602は、不正改変を阻止するために、補助記憶装置652に格納された情報を暗号化する。ROS602また、その種々のコンポーネントを別々に暗号化および有効性の検査を行う。ROS602は、エレメントが非認証的に使用されることを防ぐために制御およびデータストラクチャコンポーネントを相関させる。これらの特徴により、ROS602が、独立的にエレメントを配布し、また非安全な「他の」ＯＳ機能606とVDE機能604との統合が可能になる。

好ましい実施形態によって提供されるROS602は、例えば、アクセス制御リスト(ACL)ストラクチャなどの従来の能力の範囲を、状態遷移を含むユーザおよび処理定義されたイベントに拡張する。ROS602は、フル制御情報を、予め定義され、ユーザ定義されたアプリケーションイベントに提供し得る。これらの制御メカニズムは、「go/no-go」パーミッションを含み、またイベントの処理および/または制御において完全なフレキシビリティを許可する任意のイベント固有実行を含む。このストラクチャは、イベントが個別に制御されることを許可し、例えば、計量および予算立てが独立的な実行を使用して提供され得るようにする。例えば、ROS602は、情報の任意の細分性を制御するために、ACLストラクチャを拡張する。従来のオペレーティングシステムは、ファイルまたはリソースレベルにおいて、静的な「go/no-go」制御メカニズムを提供し；ROS602は、フレキシブルな制御ストラクチャを使用して、一般的な手法によって、制御概念の範囲を最も大きいサブエレメントから最も小さいサブエレメントまで拡張する。ROS602は、例えば、ドキュメントファイルの一段落の印刷を制御する。

好ましい実施形態によって提供されるROS602は、各コンポーネントを統治する制御情報の安全な改変および更新を許可する。制御情報はメソッドオプションなどのテンプレートフォーマットでエンドユーザに提供され得る。すると、エンドユーザは、配布者またはコンテンツ作成者によって提供されるガイドラインにおいて使用される実際の制御情報をカスタマイズし得る。好ましくは、既存の制御構成の改変および更新も、監査および制御情報を条件に制御可能なイベントである。

好ましい実施形態によって提供されるROS602は、制御ストラクチャおよび安全化された実行を使用前に有効性の検査をする。この有効性検査は、制御ストラクチャおよび実行がエンドユーザによって不正改変されていないことを確認する。

有効性検査によりまた、ROS602が、ファイルおよび他のオペレーティングシステムストラクチャのフラグメントを含むコンポーネントを安全に実行することができる。好ましい実施形態によって提供されたROS602は、オペレーティングシステムの(アクセスレベルより下の)I/Oレベルにおいて安全化の配慮を統合し、放出時に情報の「オンザフライ」復号化を提供する。これらの特徴は、従来オペレーティングシステムプラットホーム「の上にある」ＯＳ層を使用しROS602安全コンポーネントおよび情報の非安全な格納を許可する。

ROS602は、追加のオペレーティングシステム層としてホストプラットホームと高度に統合可能である。従って、ROS602は、既存のオペレーティングシステムに「追加すること」によって作成され得る。これは、装置ドライバ、およびネットワークインターフェースレベルにおいて、VDE「アドオン」のホストオペレーティングシステムへのフッキング(hooking)を伴う。また、ROS602は、VDE機能および他のオペレーティングシステム機能の両方を統合した完全に新しいオペレーティングシステムを含み得る。

まさに、権利オペレーティングシステム602を作るために、場合によっては既存のオペレーティングシステムに基づいてVDE機能を新しいオペレーティングシステムに統合するには、少なくとも３つの一般的なアプローチがある：

（１）VDE取引管理要件に基づいて、オペレーティングシステムを再設計する；

（２）VDE API機能を、既存のオペレーティングシステムにコンパイルする；および

（３）VDEインタプリタを、既存のオペレーティングシステムに統合する。

第１のアプローチは、新しいオペレーティングシステムが設計される際に、または既存のオペレーティングシステムの有意なアップグレードの計画がある場合に最も効果的に適用される。「従来」オペレーティングシステム能力とVDE能力との統合を最適かつ効率的な方法で提供する新しいオペレーティングシステムの設

計のために、設計要件リストには、VDE機能によって提供される取引管理および安全要件が加えられ得る。例えば、オペレーティングシステムのニューバージョンまたは実例の設計を担当するエンジニアは、設計アプローチ、仕様、および実際の実施を形成するための要件（仮にあるとすれば）に加えて、VDE計量／取引管理の要件を含み得る。このアプローチにより、計量／取引管理の機能性をシステム設計および実施態様におりこむことによって、VDE機能の「シームレス」な統合化および能力が得られる。

第２のアプローチは、API（アプリケーションプログラマインターフェース：Application Programmer Interface）機能の既存セットを採用すること（taking）、およびオペレーティングシステムコード内のリファレンスをVDE機能コールに取り入れることを伴う。これは、現在のWindowsオペレーティングシステムが、出発ポイントおよびWindowsオペレーティングシステムのカーネル土台の重要な部分を兼ねたDOSと共に統合される手法に類似している。このアプローチはまた、（第１のアプローチと比較した場合ほど「シームレス」ではないが）高度な「シームレス」統合化を提供する。このアプローチの利点には、オペレーティングシステムのニューバージョンまたは実例に、低コストで計量／取引管理機能性を取り入れることが（API内に具現化されている既存のコードを使用し、また、API機能アプローチの設計含意を組んで計量／取引管理機能性が取り入れられているエレメントの設計に影響を及ぼすことによって）実現されることが含まれる。

第３のアプローチは、計量／取引管理およびデータ安全に関連したVDE機能性を直接オペレーティングシステムコードに取り入れず、代わりに、新しく生成された能力をオペレーティングシステムに加えて計量／取引管理機能性を実行する点において、最初の２つのアプローチと異なる。この場合、計量／取引管理機能を含むインタプリタは、他のオペレーティングシステムコードと「スタンドアロン」モードで統合される。このインタプリタは、スクリプトまたは他のインプットを取り、計量／取引管理機能が、何を、どの順序で、どのような状況あるいは条件下で行えばいいかを決定し得る。

電子機器オペレーティングシステムに／とともにVDE機能を統合する代わりに（

またはそれに加えて)、従来のオペレーティングシステム上でランされるアプリケーションとして特定のVDE機能性を提供することが可能である。

ROSソフトウェアアーキテクチャ

図10は、好ましい実施形態によって提供される権利オペレーティングシステム(「ROS」)602のためのソフトウェア構成/アーキテクチャの一例のブロック図である。この例において、ROS602は、オペレーティングシステム(「ＯＳ」)「コア」679、ユーザアプリケーションプログラムインターフェース(「API)682、「リディレクタ」684、「インタセプト」692、ユーザ通知/例外インターフェース(Notification/Exception Interface)686、およびファイルシステム687を含む。この例のROS602はまた、１つ以上のホストイベント処理環境(「HPE」)655および/または１つ以上の安全イベント処理環境(「SPE」)503を含んでいるこれらの環境は、総称的に「保護された処理環境」650と称され得る)。

HPE655およびSPE503は、コードおよびデータ処理リソースを含む自身のオペレーティングシステムカーネル688を含み得る独立した計算および処理環境である。所与の電子機器600は、いくつものSPE503および/またはいくつものHPE655を含み得る。HPE655およびSPE503は、安全な手段で情報を処理し、ROS602のための安全処理サポートを提供し得る。例えば、それぞれが、１つ以上のVDEコンポーネントアセンブリ690に基づいて、安全な処理を行い、それぞれＯＳカーネル680に安全な処理サービスを提供し得る。

好ましい実施形態においては、SPE503は、少なくとも部分的にSPU500によって提供される安全処理環境である。従って、SPU500は、SPE503を囲むハードウェア不正改変不可能なバリア503を提供する。好ましい実施形態によって提供されるSPE503は、好ましくは：

Ｃ　小型かつコンパクトである

Ｃ　例えば、最小に構成されたSPU500などのリソース制約環境へのロードが可能である

Ｃ　動的に更新可能である

Ｃ　認証されたユーザによって拡張可能である

Ｃ　オブジェクトまたはプロシージャ環境に統合可能である

Ｃ　安全である

好ましい実施形態においては、HPE655は、例えば、電子機器CPU654汎用マイクロプロセッサもしくは他の処理システムまたは装置などSPU以外のプロセッサにサポートされた安全処理環境である。好ましい実施形態において、SPUによってハードウェアおよび/またはファームウェアに設けられる処理リソースの一部または全てを提供するためにソフトウェアを使用し得るという点で、HPE655はSPU500をエミュレートすると考えられ得る。本発明の１つの好ましい実施形態におけるHPE655は、全ての機能を有し、SPE503との完全な互換性を有している、つまり、HPE655は、SPE503が扱うことが可能なサービスコールの全てを扱うことが可能であるため、外部インターフェースの観点からは、SPEおよびHPEは「プラグ互換性」を有する（HPEはSPEほどは安全性を提供しないという点を除いて）。

HPE655は、２タイプ（安全、および非安全）で提供され得る。例えば、電子機器600が、高速汎用プロセッサまたはコンピュータの全てのリソースを用いて効率的に影響を受けにくいVDEタスクをランさせる場合には、非安全バージョンのHPE655を設置することが望ましくあり得る。そのような非安全なバージョンのHPE655は、SPE503も含むROS602の実例の監視下でランされ得る。このように、ROS602は、全ての安全処理をSPE503内でランさせ、安全性は必要としないが、HPE655をサポートする汎用コンピュータまたはプロセッサによって提供される、場合によっては大きいリソースの下で必要となり得る（またはより効率的にランする）処理のためにのみHPE655を使用し得る。非安全および安全なHPE655は、安全なSPE503とともに動作し得る。

HPE655は、（図10に示されるように）それらをより安全にするソフトウェアベース不正改変不可能バリア674を備えている。そのようなソフトウェアベース不正改変不可能バリア674は、汎用CPU654上で実行しているソフトウェアによって作成され得る。そのような「安全」なHPE655は、なお安全性を必要とする一方で、SPU500によって提供される安全の程度を要件としない処理を実行するためにROS602によって使用されることができる。これは、特にSPE503およびHPE655の両方を提

供するアーキテクチャにおいて利点が多い。SPU502が、全ての安全処理を正確に行うために使用される一方で、１つ以上のHPE655は、電子機器600内で利用可能となりうるホストプロセッサまたは他の汎用リソースを用いて追加的な安全処理(SPEよりも安全性が場合によっては低いかもしれないが)を提供するために使用され得る。そのような安全なHPE655によって、いかなるサービスも提供され得る。好ましい実施形態において、「チャネル処理」の特定の局面は、SPE503からHPE655に容易にエクスポートし得る要素が多分にあるように思われる。

HPE655によって提供されるソフトウェアベースの不正改変不可能バリア674は、例えば以下によって提供される：タイムチェックおよび/またはコード改変を導入し、デバッガを用いてカーネル688aおよび/またはコンポーネントアセンブリ690の一部を含むコードに通してステッピングする処理を複雑化する；記憶装置(例えば、ハードディスク、メモリカードなど)の欠陥マップを用いて、内部テストの値を形成し、HPE655を他の電子機器600へ移動および/またはコピーすることを妨げる；制御の流れにおいて、偽りブランチおよび他の複雑化の要素を含むカーネルコードを用いて、ディスアセンブリ、または処理の詳細を明らかにする努力から、内部処理をある程度隠蔽する；(例えば、コサイン変換の出力に基づく)「自己発生」コードを用いて、詳細および/または完全な命令シーケンスが記憶装置および/またはアクティブメモリに明確に格納される代わりに必要に応じて発生されるようにする；動作パラメータに基づくデータ値に用いられるメモリロケーションを「シャッフル」するコードを用いて、そのような値を操作する努力を困難にする；電子機器600の任意のソフトウェアおよび/またはハードウェアメモリ管理リソースを用いて、HPE655の動作を他の処理、機能などから「保護」する。そのようなソフトウェアベースの不正改変不可能バリア674は、かなり高い程度の安全性を提供し得るが、典型的に；SPU500によって(少なくともその一部が)提供されるハードウェアベース不正改変不可能バリア502ほどには安全ではない。SPU500によって提供されるようなハードウェア安全機能の援助によって、安全性がより効果的に強化されるため(またSPU500内の特定目的回路によって性能が向上するなどの他の要因のため)、多くのまたはほとんどの高位安全アプリケーシ

ョンにおいて、少なくも１つのSPE503があることが好ましい。しかし、より低い安全が許容されるおよび/またはSPU500のコストが許容されないアプリケーションにおいては、SPE503は省略され、代わりに、汎用CPU654上で実行している１つ以上の安全なHPE655によって全ての安全処理が行われ得る。関係する特定の処理において不十分な安全性が提供される場合には、VDE処理によっては、この種の安全性の低減した電子機器での実行が許可されないかもしれない。

SPE503(場合によっては、HPE655)内において完全に実行する処理のみが、真に安全であると考慮され得る。SPE503の外部にあるメモリおよび他のリソース、ならびに安全処理で使用されるコードおよび/またはデータを格納および/または処理するために使用されるHPE655は、SPE503/HPE655が非安全処理から安全処理コードおよび/またはデータを保護できない限り、暗号化形式の情報のみを受けて扱うべきである。

好ましい実施形態における、ＯＳ「コア」679は、カーネル680、RPCマネージャ732、および「オブジェクトスイッチ」734を含む。API682、HPE655、およびSPE503は、ＯＳ「コア」679を介して「イベント」メッセージを互いと通信し得る。それらはまた、ＯＳ「コア」679を通さずにメッセージを互いと直接通信し得る。

カーネル680は、電子機器600のハードウェアを管理し得る。例えば、インプット/アウトプットおよび/または、キーボード612、ディスプレイ614、「マウス」ポインティング装置および音声認識器613、モデム618、プリンタ622、およびネットワーク672のためのアダプターなど他の装置周辺機器と相互作用するために適切なドライバおよびハードウェアマネージャを提供し得る。また、カーネル680は、ROS602の残り部分(remainder)を初めにロードする役割を担当し、実行の間種々のROSタスク(および関連した下層(underlying)ハードウェアリソース)を管理し得る。ＯＳカーネル680は、また、安全データベース610およびファイルシステム687を管理およびアクセスし得る。ＯＳカーネル680はまた、アプリケーション608a(1)、608a(2)、および他のアプリケーションの実行サービスを提供する。

RPCマネージャ732は、ROS680のために、ルーチングおよびリソース管理/統合のメッセージングを行う。例えば、API682、HPE655およびSPE503からの/への、

コール」を受けおよびルートする。

オブジェクトスイッチ734は、VDEオブジェクト300の構築、解体、および他の操作を管理し得る。

好ましい実施形態における(API682またはAPIに連結した他のアプリケーションの一部とも考えられる)ユーザ通知/例外インターフェース686は、「ポップアップ(pop up)」ウィンドウ/ディスプレイをディスプレイ614に提供する。これにより、ROS602が、情報をアプリケーション608に渡して通信することなく、ユーザと直接通信することが可能になる。「VDE認識(aware)」アプリケーションではないアプリケーションに関してはユーザ通知/例外インターフェース686は、ROS602とユーザとの通信を提供し得る。

好ましい実施形態におけるAPI682は、アプリケーション608に、標準化され、文書化されたソフトウェアインタフェースを提供する。API682は、部分的に、アプリケーション608によって発生されるオペレーティングシステム「コール」を、「イベント」を特定する遠隔プロシージャコール(「RPC」)に翻訳し得る。RPCマネージャ732は、処理のために、これらのRPCを、カーネル680またはその他の場所(例えば、HPE655および/またはSPE503、または遠隔電子機器600、プロセッサ、またはVDE参加者)へルートする。またAPI682は、RPCリクエストを、特定のリクエストを受けて処理するために登録するアプリケーション608へ渡すことによってサービスし得る。

API682は、好ましくは標準化され文書化された「アプリケーションプログラミングインターフェース(Applications Programming Interface)」を提供する。アプリケーションプログラムがROS602によって提供されるサービスにアクセスするために使用できる機能コールの簡潔な(concise)セットを提供する。少なくとも1つの好ましい例において、API682は、2部分(VDE機能604とのアプリケーションプログラムインターフェース;および他のＯＳ機能606とのアプリケーションプログラムインターフェース)を含む。これらの部分は、(例えば)同じソフトウェアに組み込まれ(interwoven)、またはソフトウェアの2つ以上の離散的ピース

(discrete pieces)として提供され得る。

図11に示すアプリケーション608a(1)など、アプリケーションによっては、「VDE認識」し、従ってAPI682のこれらの部分の両方に直接アクセスし得る。図11Aは、この例を示している。「VDE認識」アプリケーションは、例えば、新たなVDEオブジェクト300の作成をリクエストし、VDEオブジェクトの使用を計量し、VDE保護形式で情報を格納するなど、ROS602に対する明示的なコールを含み得る。従って、「VDE認識」アプリケーションは、ROS602によって提供されるVDE機能性を開始(例によっては、向上および/または拡張)することができる。さらに、「VDE認識」アプリケーションは、ユーザとROS602との間により直接的なインターフェースを(例えば、ユーザ通知/例外インターフェース686によって提供される「ポップアップ」ディスプレイを抑制さもなくば省き、代わりに、アプリケーションおよびROSメッセージを統合する、より「シームレス」なインターフェースを提供することによって)提供し得る。

図11Bに示されるアプリケーション608bのような他のアプリケーションは、「VDE認識」し得ず、従って、API682によって提供されるVDE機能604に対するインターフェースにどのように直接アクセスするかを「知」らないかもしれない。これを提供するために、ROS602は、そのような「非VDE認識」アプリケーション608bがVDEオブジェクト300および機能604にアクセス可能にする「リディレクタ」684を含み得る。好ましい実施形態におけるリディレクタ684は、「他のＯＳ機能」606に向けられたＯＳコールを、「VDE機能」604へのコールへと翻訳する。１つの簡単な例として、リディレクタ684は、アプリケーション608bからの「ファイルを開く」というコールをインタセプトし、開かれるべきファイルがVDEコンテナ300内に含まれているか否かを決定し、含まれていれば、VDEコンテナを開くためにファイルシステム687への適切なVDE機能コールを発生する(また、場合によっては、VDEオブジェクト300に格納され得るファイルネームを決定し、VDEオブジェクト300に関連した制御ストラクチャを確立し、VDEオブジェクト300などへの登録を行うために、HPE655および/またはSPE503へのイベントを発生する)。この例において、リディレクタ684がない場合、608bなどの非VDE認識アプリケーションは、他のＯＳ機

能606とのインターフェースを提供するAPI682の一部のみにしかアクセスできず、従ってどのVDE機能にもアクセスできない。

リディレクタ684のこの「翻訳」機能は、「トランスペアレンシ」を提供する。これは、VDE機能604への１つ以上のコールを発生することに伴う複雑性、および細部にアプリケーションが影響されることなしに、VDE機能をアプリケーション608(b)に「トランスペアレト」な方法で設けられるようにする。ROS602のこの「トランスペアレンシ」の特徴の局面は、少なくとも以下の２つの重要な利点を有している：

（ａ）VDE機能604用に特別に書かれたわけではないアプリケーション（「非VDE認識アプリケーション」）でも、重要なVDE機能とアクセスすることを可能にする；および

（ｂ）アプリケーションとROS602との間のインターフェースの複雑さを低減する。

第２の利点（複雑性の低減）は、アプリケーション作成者が容易にアプリケーションを作成できるようにするため、たとえ「VDE認識」アプリケーション608a(2)であっても、VDE機能604を呼び出すコールの一部が「他のＯＳ機能」コールレベルでリクエストされ、リディレクタ684(この場合、リディレクタ684はAPI682の一部と考えられる)によってVDE機能コールに「翻訳」されるように設計され得る。図11Cは、これを例示する。VDE機能604を呼び出す他のコールは、リディレクタ684による翻訳なしに直接渡され得る。

図10を再度参照すると、ROS620はまた、１つ以上のリアルタイムデータフィード694を転送および/または受信し（これは、例えばケーブル628を介して行われ得る）、またそのような１つ以上のデータフィードを適切にルートする一方で、電子機器600に送信および/または受信されるリアルタイムデータのための「翻訳」機能を提供して、この種の情報にリディレクタ684によって得られるトランスペアレンシと同様の「トランスペアレンシ」を付与する（および/または１つ以上のリアルタイムデータフィードを生成し得る）「インタセプタ」692を含み得る。

安全ROSコンポーネントおよびコンポーネントアセンブリ

前述したように、好ましい実施形態におけるROS602は、コンポーネントベースアーキテクチャである。ROS VDE機能604は、区分され、独立的にロード可能かつ実行可能な「コンポーネントアセンブリ」690に基づき得る。これらのコンポーネントアセンブリ690は、独立的に安全に送達可能である。好ましい実施形態によって提供されるコンポーネントアセンブリ690は、自ら独立的に送達可能なコードおよびデータエレメントを含む。従って、好ましい実施形態により提供される各コンポーネントアセンブリ690は、VDE安全サブシステムの間でVDE安全通信技術を用いて通信され得る、独立的に安全に送達可能なエレメントを含んでいる。

これらのコンポーネントアセンブリ690は、ROS602によって提供される基本機能ユニットである。コンポーネントアセンブリ690は、オペレーティングシステムまたはアプリケーションタスクを行うために実行される。従って、あるコンポーネントアセンブリ690は、ROSオペレーティングシステム602の一部と考えられ、他のコンポーネントアセンブリは、オペレーションシステムのサポートの下でランする「アプリケーション」と考えられ得る。「アプリケーション」および「オペレーティングシステム」を取り入れたいかなるシステムにおいても、システム全体のこれらの局面の間の境界は曖昧であり得る。例えば、（コンテンツコンテナのストラクチャおよび/または他の属性を決定するなどの）一般的に使用される「アプリケーション」機能が、オペレーティングシステムに取り入れられ得る。さらに、（タスク管理、またはメモリアローケーションなどの）「オペレーティングシステム」機能は、新たなアプリケーションに改変されおよび/または置き換えられ得る。好ましい実施形態のROS602において、コンポーネントアセンブリ690が、ユーザが意図する活性化を遂行するために一般的なつなぎ（thread）が必要となる、このつなぎは場合によっては「アプリケーション的」であり、また場合によっては「オペレーションシステム的」である機能を提供することである。

コンポーネント690は、好ましくは、容易に分離可能かつ独立的にロード可能なように設計される。ROS602は、コンポーネントアセンブリを（例えば、SPE503および/またはHPE655などの安全な動作環境において）ロードおよび実行する前に、これらのエレメントを一緒にして、実行可能なコンポーネントアセンブリ690

を

構成する。ROS602は、実行前および/または実行の間に、エレメントを自動的かつ安全にコンポーネントアセンブリ690を構成するために必要な情報を含むエレメント識別および照会メカニズムを提供する。

コンポーネントアセンブリ690を形成するために使用されるROS602アプリケーションストラクチャおよび制御パラメータは、異なるパーティによって提供され得る。コンポーネントアセンブリ690を形成するコンポーネントは、独立的かつ安全に送達可能であるために、異なる時間および/または異なるパーティによって送達され得る(「送達」は局所VDE安全サブシステムにおいて実施され得る、すなわち、改変された制御情報セットの用意のために参加者を取り扱うコンテンツ制御情報のチェインによる、制御情報のそのような安全なサブシステムの使用を通しての依頼は、独立的かつ安全な送達を構成する)。例えば、コンテンツ作成者は、VDEオブジェクト300に含まれるコンテンツをライセンス認可するために必要な状況を定義するROS602アプリケーションを作成し得る。このアプリケーションは、他のパーティによって提供されるストラクチャを照会し得る。そのような照会は、例えば、ユーザ作業を計量するためにはコンテンツ作成者ストラクチャを使用し;コンテンツ配布取引きの金融関連部分(例えば、制御ストラクチャになくてはならない貸し方予算を定義して、許可された者によって行われなければならない信用貸しする価値、監査処理を確立するなど)を扱うためには金融プロバイダー(financial provider)によって作成/所有される構成を使用する制御パスの形態を取り得る。他の例として、配布者は、異なるユーザへの値段を規定する異なるデータエレメントを送達することによって、1名のユーザに対して他のユーザよりも好都合な値段を付け得る。安全かつ独立的に送達可能な多数パーティ用の制御情報をサポートするこの属性は、電子商取引、すなわち、コンテンツクリエータ、他のコンテンツプロバイダー、金融サービスプロバイダー、および/またはユーザなどの独立パーティの集合(collection)の要件を示すコンテンツおよび/または機器制御情報セットの定義を可能にするために必須である。

好ましい実施形態において、ROS602は、コンテンツパラメータ(例えば、オブ

ジェクト、ユーザ)に部分的に基づき、安全かつ独立的に送達可能な、エレメントをコンポーネントアセンブリ690を構成する。従って、例えば、ROS602は、同じVDEオブジェクト300に同じタスクを行う異なるユーザのために、異なるエレメントを一緒に安全に構成し、異なるコンポーネントアセンブリ690に形成し得る。同様に、ROS602は、異なるVDEオブジェクト300に同じタスクを行う同じユーザのために、１つ以上の同じコンポーネントを含み得るすなわち再利用し得る異なるエレメントセットを構成して、異なるコンポーネントアセンブリ690を形成し得る。

自らが独立的にロード可能かつ実行可能なコンポーネントアセンブリ690である１つ以上のコンポーネント「サブアセンブリ」を、コンポーネントアセンブリ690が含み得るという点から、ROS602によって提供されるコンポーネントアセンブリ組織(organization)は「再帰的(recursive)」である。これらのコンポーネント「サブアセンブリ」は、また１つ以上のコンポーネント「サブサブアセンブリ」からなり得る。一般的な場合において、コンポーネントアセンブリ690は、Ｎレベルのコンポーネントサブアセンブリを含み得る。

従って、例えば、コンポーネントアセンブリ690(ｋ)は、コンポーネントサブアセンブリ690(ｋ+1)を含み得る。またコンポーネントサブアセンブリ690(ｋ+1)は、コンポーネントサブサブアセンブリ690(3)を含み得、以下同様にＮレベルサブアセンブリ690(ｋ+Ｎ)まで続く。他のコンポーネントアセンブリからコンポーネントアセンブリ690を築く(build)ROS602の能力は、例えば、コード/データ再利用性、および異なるパーティがコンポーネント全体の異なる部分を管理することを可能にする能力の点で多大な利点を提供する。

好ましい実施形態における各コンポーネントアセンブリ690は、異なるコンポーネントからなる。図１１D～１１Hは、図１１Ｉに示されるコンポーネントアセンブリ690(ｋ)を形成するために構成され得る種々の異なるコンポーネントの抽象描写である。これらの同様のコンポーネントは、異なる手法(例えば、より多くのコンポーネントまたはより少ないコンポーネント)で構成されて、完全に異なる機能作用を提供する異なるコンポーネントアセンブリ690を形成し得る。図１１Ｊは、同

じコンポーネントを異なる手法で(例えば、コンポーネントを追加して)共に合わせ、異なるコンポーネントアセンブリ690(j)を形成した場合の抽象描写である。コンポーネントアセンブリ690(k)および690(j)はそれぞれ、ROS602によって規定された「チャネル」594と嵌合する共通部(common feature)691を含む。この「チャネル」594はコンポーネントアセンブリ690を組合せ、(残りの)ROS602とインターフェースさせる。

ROS602は、コンポーネントアセンブリ690を安全に生成する。図11Iおよび11Jに視覚的に示されるように、コンポーネントアセンブリ690を含む異なるエレメントは、エレメントを作成しおよび/またはコンポーネントアセンブリを特定したVDE参加者によって意図されたようにしか「嵌合」しないようにし得る。ROS602は、非承認者がエレメントを改変すること、また非承認者がエレメントを置換えることを防ぐ安全保護を含む。非承認者が、図11D～11Hに示されるエレメントの1つと同じ「形」を有する新しいエレメントを作り、元のエレメントをその新しいエレメントと置換えることを試みることが考えられる。図11Hに示されるエレメントの1つが、VDEオブジェクト300内のコンテンツを使用するための値段を確立するものとする。非承認者が、自らの「値段」エレメントを、VDEコンテンツ配布者によって意図される値段エレメントとを置換え得るとしたら、その者はコンテンツ配布者が請求しようとしている値段の代わりにゼロという値段を付けることができる。同様に、エレメントが電子クレジットカードを確立している場合、異なるエレメントと置換えることが可能であれば、人が自分の使用額を他人の(または存在しない)クレジットカードに請求することができ、大損害な結果を招き得る。これらは、特定のコンポーネントアセンブリ690が安全に形成されることを確実にするROS602の重要性を示す単なる数少ない例でしかない。ROS602は、コンポーネントアセンブリ690の安全な取り扱いおよび実行に関する多くの「脅威」に対する広い保護範囲を提供する。

好ましい実施形態において、ROS602は、以下のタイプのエレメントに基づいてコンポーネントアセンブリ690を構成する：

パーミッション記録(「PERC」)808；

メソッド「コア」1000；

ロードモジュール1100；

データエレメント（例えば、ユーザデータエレメント（「UDE」）1200およびメソッドデータエレメント（「MDE」）1202）；および

他のコンポーネントアセンブリ690。

簡潔に言えば、好ましい実施形態によって提供されるPERC808は、ROS602に付随した（identifies to）VDEオブジェクト300に対応する記録であり、とりわけエレメントROSは共に組み合わせられてコンポーネントアセンブリ690を形成する。従って、PERC808は実質的に、どのエレメントとROS602とが共に構成されてコンポーネントアセンブリを形成するのか、またどのようにエレメントを共に接続するのかを特定する「構成命令のリスト」または「プラン」を含む。PERC808は、自らデータまたはコンポーネントアセンブリ690の一部となる他のエレメントを含み得る。

PERC808は、１つ以上のメソッド「コア」1000Nを照会し得る。メソッド「コア」1000Nは、基本「メソッド」1000（例えば、「制御」、「課金」、「計量」など）を定義し得る。

好ましい実施形態において、「メソッド」1000は、１つ以上の電子機器600の動作に関係した基本命令の集合、および基本命令に関連した情報であり、実施および/または実施の準備における使用のコンテクスト、データ、要件および/または関係を提供する。基本命令は、例えば、以下を含み得る：

Ｃ　コンピュータのプログラミングにおいて一般的に使用されるタイプの機械コード；コンピュータ上で動作しているインタプリタまたは他の命令処理プログラムによって使用される疑似コード；

Ｃ　電子機器600とともに使用される、電子的に示される論理動作のシーケンス；

Ｃ　または、技術分野において一般的にその用語が理解されるように、命令、ソースコード、オブジェクトコード、および/または疑似コードの他の電子的な表現。

基本命令に関連する情報は、例えば、基本命令に本質的に伴うデータ、例えば、組み合わされた基本命令のための識別子、および本質データ、アドレス、定数などを含み得る。情報はまた、例えば、以下の内１つ以上を含み得る：

C　アクセス、相関、および/または有効性検査目的のための関連する基本命令および本質データを識別する情報；

C　基本命令および本質データの使用のための必須のおよび/または任意のパラメータ；

C　他のメソッドとの関係を定義する情報；

C　データ値、情報分野などを含み得るデータエレメント；

C　データエレメント、基本命令、および/または本質データの関係を特定および/または定義する情報；

C　外部データエレメントとの関係を特定する情報；

C　存在すれば、内部および外部データエレメント、メソッドなどの関係を特定する情報；ならびに

C　必要であれば、追加命令および/または本質データを含むメソッドのユーザによって意図される基本命令および本質データを完了するための動作、または完了させる試みに必要とされる追加情報。

メソッドに関連したそのような情報はその一部分またはその全体が、基本命令および本質データとは別に格納され得る。これらのコンポーネントが別々に格納された場合でも、メソッドは、所与の時点において基本命令および本質データの１つ以上のセットがアクセス可能であるか否かに関わらず、他の情報、ならびに基本命令および本質データの１つ以上のセット（後者は、他の情報が基本命令および本質データの１つ以上のセットを参照するために含まれる）を含み、封じ（encompass）得る。

メソッドコア1000'は、「事象コード」によってパラメータ表示されて異なる事象に対して異なるメソッドで応答することを可能にし得る。例えば、METERメソッドは、計量データ構成に使用情報を格納して「使用」事象に応答し得る。同じMETERメソッドは、VDE情報交換所または他のVDE参加者へ計量データ構成を報告し

て、「管理」事象に対して応答し得る。

好ましい実施形態において、メソッドコア1000'は、明確にまたは参照することによって、１つ以上の「ロードモジュール」1100および1つ以上のデータエレメント(UDE1200、MDE1202)を「含み」得る。好ましい実施形態において、「ロードモジュール」1100は、基本命令および本質データを反映するメソッドの一部である。

好ましい実施形態におけるロードモジュール1100は、実行可能なコードを含み、またその実行可能なコードに関連したデータエレメント(「DTD」1108)を含み得る。好ましい実施形態において、ロードモジュール1100は、メソッドによって定義された処理を行うために実際にハードウェアによって「実行される」プログラム命令を与える。ロードモジュール1100は、他のロードモジュールを含むか、または参照し得る。

好ましい実施形態におけるロードモジュール1100は、個々のロードモジュールが再エンターおよび再利用可能であるように、モジュラー化され、および「コードピュア(code pure)」である。コンポーネント690が動的に更新することができるために、それらはグローバル公開ネームスペース(global public name space)内で個々にアドレスされることが可能であり得る。これらの設計上の目標の観点から、ロードモジュール1100は、好ましくは、小さく、個々に名指しされ(named)、アドレス可能なコード(およびコード状)ピュアモジュールである。単一のメソッドは、異なるプラットホームにおいて同じまたは類似の機能を行う異なるロードモジュール1100を提供し、異なる電子機器の幅広い範囲にわたってメソッドを規模変更可能および/または移植可能にし得る。

UDE1200およびMDE1202は、実行可能なコンポーネントアセンブリ690への入力または実行可能なコンポーネントアセンブリ690からの出力のためのデータ(またはそのような入力および/または出力を記述するデータ)を格納し得る。好ましい実施形態において、UDE1200はユーザ依存し、MDE1202はユーザから独立し得る。

図11Eに示されたコンポーネントアセンブリ例690(k)は、メソッドコア1000'、UDE1200aおよび1200b、MDE1202、ロードモジュール1100a～1100d、さらにコンポ

ーネントアセンブリ690(ｋ＋１)を含む。前述したように、PERC808(k)は、とりわけ、コンポーネントアセンブリ690(k)のための「構成命令」を定義し、コンポーネントアセンブリを作成するために構成されたコンポーネントのいくらかを、部分的または全体的に含み、または参照し得る。

この例に示されるロードモジュール1100bの１つは、自らが複数のロードモジュール1100cおよび1100dを含む。この例のいくつかのロードモジュール(例えば、1100a、1100d)は、１つ以上の「DTD」データエレメント1108(例えば、1108a、1108

b)を含む。「DTD」データエレメント1108は、例えば、MDE1202および/またはUDE1200aおよび1200bに含まれるデータエレメントのロードモジュール1100aを知らせるために使用され得る。さらに、DTD1108は、１つ以上のロードモジュール1100、またはその他のコンポーネントエレメントに必要とされるおよび/または操作される情報とユーザに知らせるために使用されるアプリケーションの一部を形成する局面として使用され得る。そのようなアプリケーションプログラムはまた、UDE1200、MDE1202、または他のコンポーネントエレメント、サブアセンブリなどを作成し、および/または操作するための機能を含み得る。

コンポーネントアセンブリ690内のコンポーネントは、異なるコンポーネントアセンブリを形成するために「再利用」され得る。前述したように、図11Fは、再利用されるコンポーネントアセンブリ690(k)を構成するために使用されたコンポーネントと同じコンポーネントの一例を示す抽象的な描写であり、(例えば、異なるPERC808(1)が提供する「構成命令」の異なるセットによって特定されるいくつかの追加のコンポーネントとともに)異なるコンポーネントアセンブリ690(1)を形成する。コンポーネントアセンブリ690(k)を形成するために使用されたコンポーネントのいくつかと同じコンポーネントからコンポーネントアセンブリ690(1)が形成されるにも関わらず、これらの２つのコンポーネントアセンブリは完全に異なる処理を完全に異なるメソッドで行いうる。

前述したように、ROS602は、コンポーネントアセンブリ690の安全を確実にするために何層かの安全層を提供する。重要な安全層の内の１つは、例えばSPU500

内に設置される安全な実行スペースにおいてのみ、特定のコンポーネントアセンブリ690が形成され、ロードされ、実行されることを確実にすることに関する。コンポーネント690および/またはそれらを含むエレメントは、局所SPU500が発生した鍵および/または配布者の供給した鍵を使用して暗号化された外部媒体に格納され得る。

ROS602はまた、置換による不正改変を検出するために、ロード可能なコンポーネントアセンブリ690内において使用され得るタギング(tagging)および順序づけスキームを提供する。コンポーネントアセンブリ690を含む各エレメントは、SPU500にロードされ、暗号化/復号化エンジン522を用いて復号化され、その後適切

なエレメントがロードされたことを確実にするためにテスト/比較され得る。非承認な置換がなかったことを確実にするために、いくつかの独立的な比較が用いられ得る。例えば、エレメントIDの公開および秘密コピーを比較し、それらが同じであることを確実にし、エレメントの著しい置換を防ぎ得る。さらに、ロード可能なエレメントの暗号化層の下に格納された有効性検査/相関タグを、それがリクエスト処理によって提供された一つ以上のタグと一致することを確実にするために比較し得る。これにより、非承認な情報の使用を防ぐことができる。第3の保護として、SPU500の予期する対応タグ値と一致することを確実にする為にロード可能なエレメントの暗号化層の下に格納された装置割り当てタグ(device assigned tag)(例えば、シーケンス番号)がチェックされる。これにより、古いエレメントの置換を防ぐ。典型的に、有効性検査/相関タグは安全ラッパ(wrappers)にのみ渡され、SPU500の外にこの情報が普通文書で曝される(plaintext exposure)ことを防ぐ。

ROS602の安全コンポーネントベースアーキテクチャは重要な利点を有している。例えば、比較的低コストのSPU500によって提供されるような限られたリソース実行環境を許容する。また、非常に高レベルの構成性(configurability)も提供する。実際、ROS602は、ほとんど無限に多様なコンテンツタイプ、コンテンツプロバイダー目的、取引タイプおよびクライアント要件を許容する。さらに、特定のオブジェクトおよびユーザに基づいた実行時に、独立的に送達可能なコンポー

ネントを動的に構成する能力は、高い度合いのフレキシビリティを提供し、配布されたデータベース、処理、および実行環境を容易または可能にする。

ROS602によって提供されるコンポーネントベースアーキテクチャの利点の局面の1つは、時間の間ずっと機能性および能力を「計画的に実施(stage)」する能力に関係する。設計されれば、ROS602の実施は制限のある(finite)タスクである。市場実体が対応したVDEアプリケーション機能性の実施を要求するまで、機能性の多くの局面は、未開発のままであり得る。その結果、初期製品実施の投資および複雑性が抑えられ得る。ROS602によって提供される、承認、認証、および人工知能アプリケーションに関する能力の全範囲を「表面化」する過程は時間をかけて実現され得る。また、すでに設計されたROS602の機能性は、変更の必要または要求に適合するために常に変更または向上され得る。

権利オペレーティングシステム602アーキテクチャのより詳細な議論

図12は、図10に示されるROS602の詳細なアーキテクチャの一例を示す。ROS602は、商用データベースマネージャ730および外部オブジェクト容器728を含むファイルシステム687を含み得る。商用データベースマネージャ730は、安全データベース610を維持し得る。オブジェクト容器728は、VDEオブジェクト300を格納し、VDEオブジェクト300へのアクセスを提供し、および/またはVDEオブジェクト300を維持する。

図12はまた、ROS602が、1つ以上のSPE503および/または1つ以上のHPE655を提供し得ることを示している。前述されたように、HPE655は、SPU500装置を「エミュレート」し、そのようなHPE655は、より高い処理量を必要とするシステムのために、物理的なSPU500の代わりに(またはそれに加えて)統合され得る。HPE655はオペレーティングシステム安全化によって保護され、高信頼の安全処理を提供し得ないかもしれないため、いくらかの安全性は消えうる。従って、好ましい実施形態において、少なくとも安全性の高いアプリケーションのために、全ての安全化処理は、電子機器600の他の場所において動作しているソフトウェアを使用するHPE655よりも、物理的なSPU500内に実行スペースを有するSPE503内で実施されるべきである。

前述されたように、ROS602の３つの基本コンポーネントは、カーネル680、遠隔プロシージャコール(RPC)マネージャ732およびオブジェクトスイッチ734である。これらのコンポーネント、およびそれらがROS602の他の部分と相互作用する手法を以下に記載する。

カーネル680

カーネル680は、電子機器600の基本ハードウェアリソースを管理し、ROS602によって提供される基本タスキング(tasking)を制御する。好ましい実施形態におけるカーネル680は、メモリマネージャ680a、タスクマネージャ680b、およびI/Oマネージャ680cを含み得る。タスクマネージャ680bは、実行可能なタスクを初期化しおよび/またはその初期化を管理し、ROS602がランしているプロセッサ(例えば、図８に示されるCPU654)によってそれらが実行されるようにスケジュールし得る。例えば、タスクマネージャ680bは、ROS602の他の部分をロードするブートストラップローダ(loader)を含む、または伴い得る。タスクマネージャ680bは、アプリケーションプログラム608を伴うタスクを含む、ROS602に関する全てのタスキングを管理し得る。メモリマネージャ680aは、電子機器600のメモリ(例えば、図８に示されるRAM656)のアロケーション、ディアロケーション、共有、および/または使用を管理し、例えば、電子機器および/または関連アプリケーションに必要とされれば仮想メモリ能力を提供し得る。I/Oマネージャ680cは、ROS602へのインプット/ROS602からのアウトプットの全てを管理し、物理的な装置との通信および相互作用を提供するドライバおよび他のハードウェアマネージャと相互作用し得る。

RPCマネージャ732

好ましい実施形態におけるROS602は、サービスベースの遠隔プロシージャコールアーキテクチャ/インターフェースの周囲に設計される。ROS602によって行われる全機能が、サービスおよび共有情報をリクエストするためにこの共通インターフェースを使用し得る。例えば、SPE503は、１つ以上のRPCベースサービスのための処理を提供する。SPU500をサポートすることに加えて、RPCインターフェースは、外部サービスの動的な統合を可能にし、既存のオペレーティングシス

テムコンポーネントを使用した構成オプションのアレイ(OSlan array of configuration options)を提供する。ROS602はまた、配布されたおよび/または遠隔的な処理をシームレスに提供するために、RPCインターフェースを介して外部サービスと通信する。ROS602の小規模変更の事例においては、リソースを保存するために、比較的簡単なメッセージを渡すIPCプロトコルを使用し得る。これは、ROS602サービスの構成性を限定し得るが、この可能な限定は、電子機器によっては許容され得る。

RPC構成は、どの場所にサービスが物理的に提供されるのか、どのシステムまたは装置がリクエストをサービスするのか、またはどのようにサービスリクエストが遂行されるのかをコール処理において知ることまたは特定することなしに、サービスがコール/リクエストされることを可能にする。この機能は、特定のアプリケーションのために規模変更および/またはカスタマイズされ得るサービスの群(families)をサポートする。サービスリクエストは、ローカルサービスシステムによって継続されサービスされ得る場合と同じくらい容易に、異なるプロセッサおよび/または異なるサイトによって、継続されサービスされ得る。好ましい実施形態において、オペレーティングシステムの中または外にサービスをリクエストするために、同じRPCインターフェースがROS602によって用いられているため、配布されたおよび/または遠隔的な処理のためのリクエストは、その上に(overhead)追加のオペレーティングシステムを実質的に必要としない。遠隔処理は、局所ベースサービスをリクエストするためにROS602によって使用される同じサービスコールの一部として，容易かつ簡単に統合される。さらに、標準RPCインターフェース(RSI)の使用により、ROS602がモジュラー化され、異なるモジュールが、オペレーションシステムの残りとの標準化されたインターフェースを提示する(presenting)ことを可能にする。そのようなモジュラー化および標準化されたインタフェースにより、異なる販売者/オペレーティングシステムプログラマーがオペレーティングシステムの異なる部分を独立的に作成し、要求および/またはプラットホームに基づいて、ROS602の機能性がフレキシブルに更新および/または変更されることを可能にする。

RPCマネージャ732は、RPCインターフェースを管理する。RPCマネージャ732は、サービスリクエスタからサービスリクエストを、１つ以上の遠隔プロシージャコール（RPC）の形態で受け、サービスリクエストを、リクエストをサービスできるサービスプロバイダーにルートする。例えば、権利オペレーティングシステム602が、ユーザアプリケーションからユーザAPI682を介してリクエストを受けた場合、RPCマネージャ732は、「RPCサービスインターフェース」（「RSI」）を介してサービスリクエストを適切なサービスにルートし得る。RSIは、RPCマネージャ732と、サービスリクエスタと、リクエストを受容しサービスするリソースとのインターフェースである。

RPCインターフェース（RSI）は、好ましい実施形態において、いくつかの主要ROS602サブシステムのために使用される。

好ましい実施形態におけるROS602によって提供されるRPCサービスは、サブサービス、すなわちそれぞれが個別にRPCマネージャ732によってトラック（track）され得る特定サービスの個別の事例、に分けられる。このメカニズムにより、実施のスペック（spectrum）にわたる共通インターフェースを維持しながら、比較的高い処理量システム上で多数の特定サービスの事例が許容される。サブサービスコンセプトは、多数のプロセッサ、多数のSPE503、多数のHPE655、および多数の通信サービスをサポートするにまで拡張する。

好ましい実施形態のROS602は、以下のRPCベースサービスプロバイダ/リクエスタ（それぞれ、RPCマネージャ732と通信するRPCインターフェースまたは「RSI」を有する）を提供する：

SPE装置ドライバ736（このSPE装置ドライバは、好ましい実施形態においてSPE503に接続される）；

HPE装置ドライバ738（このHPE装置ドライバは、好ましい実施形態においてHPE738と接続される）；

通知サービス740（この通知サービスは、好ましい実施形態においてユーザ通知インターフェース686と接続される）；

APIサービス742（このAPIサービスは、好ましい実施形態においてユーザAPI682

と接続されている）；

リディレクタ684；

安全データベース（ファイル）マネージャ744（この安全データベースまたはファイルマネージャ744は、キャッシュマネージャ746、データベースインターフェース748、およびデータベースドライバ750を介して、商用データベースマネージャ730および安全ファイル610と接続および相互作用し得る）；

ネームサービスマネージャ752；

出力管理オブジェクトマネージャ754；

入力管理オブジェクトマネージャ756；

オブジェクトスイッチ734へのゲートウェイ734（これは、RPCマネージャ732とオブジェクトスイッチ734との直接通信に使用されるパスである）；および

通信マネージャ776。

HPE655、SPE503、ユーザ通知686、API742、およびリディレクタ684によって提供されるサービスのタイプは、すでに前述した。以下に、OSリソース744、752、754、756、および776によって提供されるサービスのタイプの簡単な説明をする：

安全データベースマネージャ744は、安全データベース610へのアクセスのためのリクエストをサービスする；

ネームサービスマネージャ752は、ユーザ、ホスト、またはサービスIDに関連したリクエストをサービスする；

出力管理オブジェクトマネージャ754は、出力管理オブジェクトに関連したリクエストをサービスする；

入力管理オブジェクトマネージャ756は、入力管理オブジェクトに関連したリクエストをサービスする；および

通信マネージャ776は、電子機器600と外界との通信に関連したリクエストをサービスする。

オブジェクトスイッチ734

オブジェクトスイッチ734は、VDEオブジェクト300を（局所的にも遠隔的にも）

扱い、制御し、通信する。好ましい実施形態においては、オブジェクトスイッチは、以下のエレメントを含み得る：

ストリームルータ758；

(リアルタイムデータフィード694に接続され得る)リアルタイムストリームインターフェース760；

時間依存的ストリームインターフェース762；

インタセプト692；

コンテナマネージャ764；

１つ以上のルーティングテーブル766；および

バッファリング/格納768。

ストリームルータ758は、リアルタイムストリームインターフェース760および時間依存ストリームインターフェース762によってそれぞれ扱われるリアルタイムおよび時間依存データストリームへ/からルートする。インターセプト692は、例えばリアルタイムフィード694などのリアルタイム情報ストリームを伴うI/Oリクエストをインターセプトする。ストリームルータ758によって行われるルーティングは、ルーティングテーブル766によって決定され得る。バッファリング/格納768は、一時的な蓄積交換(store-and-forward)、バッファリング、および関連サービスを提供する。コンテナマネージャ764は(代表的にはSPE503と共に)、オブジェクトの一部をコンストラクトし、ディコンストラクトし、突き止めるなど、VDEオブジェクト300を処理し得る。

オブジェクトスイッチ734は、オブジェクトスイッチインターフェース(「OSI」)を介して、ROS602の他の部分と通信する。好ましい実施形態において、オブジェクトスイッチインターフェースは、例えば、Unixソケット用のインターフェースに類似し得る。図12に示される各「OSI」インターフェースは、オブジェクトスイッチ734と通信する能力を有している。

ROS602は、以下のオブジェクトスイッチサービスプロバイダー/リソース(それぞれ「OSI」を介してオブジェクトスイッチ734と通信できる)を含んでいる：

出力管理オブジェクトマネージャ754；

人力管理オブジェクトマネージャ７５６；

ゲートウェイ７３４(RPCマネージャ７３２が、例えばサービスを提供および/またはリクエストするために、オブジェクトスイッチ７３４またはOSIを有する他のエレメントと通信し得るように、RPCコールをオブジェクトスイッチコールにまたはその逆に翻訳する)；

外部サービスマネージャ７７２；

オブジェクト実行依頼マネージャ７７４；および

通信マネージャ７７６。

簡単にいえば、

オブジェクト容器マネージャ７７０は、オブジェクト容器７２８へのアクセスに関連したサービスを提供する；

外部サービスマネージャ７７２は、ネットワークリソースまたは他のサイトからなど、外部的にリクエストおよび受けとることに関連したサービスを提供する；

オブジェクト実行依頼マネージャ７７４は、ユーザアプリケーションがどのようにオブジェクトスイッチ７３４と相互作用するのかということに関連したサービスを提供する(オブジェクト実行依頼マネージャは、アプリケーションプログラム６０８へのインターフェースを提供するため、ユーザAPI６８２の一部と考えられ得る)；および

通信マネージャ７７６は、外界との通信に関連したサービスを提供する。

好ましい実施形態において、通信マネージャ７７６は、ネットワークマネージャ７８０およびメールゲートウェイ(マネージャ)７８２を含み得る。メールゲートウェイ７８２は、例えば、オブジェクトスイッチ７３４と外界電子メールサービスとの間に自動的にVDE関連電子メールをルートするために、１つ以上のメールフィルタ７８４を含み得る。外部サービスマネージャ７７２は、サービストランスポート層７８６を介して、通信マネージャ７７６とインターフェースをとり得る。サービストランスポート層７８６aは、外部サービスマネージャ７７２が、サービストランスポート層７８６を用いて管理された種々のプロトコルを用いて、外部コンピュータおよびシステムと通信することを可能にし得る。

図12に示されるROS680の種々のサブシステムの特性およびそれに対するインタフェースを以下に詳細に説明する。

RPCマネージャ732およびそのRPCサービスインターフェース

前述されたように、ROS602によって提供される基本システムサービスは、RPCサービスインターフェース(RSI)を使用することによって呼び出される。このRPCサービスインターフェースは、ROS602によって提供される異なるサービスシステムおよびサブシステムのための包括的な、標準化されたインターフェースを提供する。

RPCマネージャ732は、RPCのリクエストするサービスを適切なRPCサービスインターフェースにルートする。好ましい実施形態において、RPCコールを受け取る

と同時に、RPCマネージャ732は、リクエストをサービスする１つ以上のサービスマネージャを決定する。RPCマネージャ732は次いで、適切なサービスマネージャによる作業のために、サービスリクエストを適切なサービスへ(サービスに関連したRSIを介して)ルートする。

例えば、SPE503がリクエストをサービスする場合、RPCマネージャ732は、リクエストをRSI736aへルートし、RSI736aはリクエストをSPE装置ドライバ736へ渡し、SPEへ進む。同様に、HPE655がリクエストをサービスする場合には、RPCマネージャ732は、リクエストをRSI738aにルートし、HPEへ進む。１つの好ましい実施形態において、RSI736aおよび738aが同じRSIの異なる事例となるように、SPE503およびHPE655は本質的に同じサービスを行い得る。いったんサービスリクエストがSPE503(またはHPE655)に受け取られると、典型的にSPE(またはHPE)は、自らの内部RPCマネージャを用いてリクエストを内部的にディスパッチする(後で簡単に説明される)。SPE503およびHPE655内での処理はまた、RPCリクエストを発生し得る。これらのリクエストは、SPE/HPEによって内部処理され、内部的にサービス可能でない場合には、RPCマネージャ732によってディスパッチするためにSPE/HPEの外に渡される。

遠隔(および局所)プロシージャコールは、RPCサービステーブルを使用してRPCマネージャ732によってディスパッチされ得る。RPCサービステーブルは、特定

のサービスのためのリクエストが処理のためにどこにルートされるかを示す。好ましい実施形態におけるRPCサービステーブルの各ロウは、サービスID、サービスのロケーション、およびリクエストをサービスするために制御が渡されるアドレスを含む。RPCサービステーブルはまた、RPCディスパッチャのどの事例がサービスを制御するかを示す制御情報を含み得る。RPCマネージャ732、ならびに取り付けられたSPE503およびHPE655のいずれも、RPCサービステーブルの対称的なコピーを有し得る。RPCサービスが、RPCサービステーブルにおいて見つからなかった場合、拒絶されるかもしくは遠隔サービスのために外部サービスマネージャ772に渡される。

RPCマネージャ732が、RPCサービステーブル内のリクエストに対応するロウを見つけたとすると、リクエストを適切なRSIにディスパッチし得る。受け取るRSIは、(RPCサービステーブル内のリクエストを探索(look-up)したかもしれない)RPCマネージャ732からのリクエストを受容し、特定サービスに関連した内部性質に従ってそのリクエストを処理する。

好ましい実施形態において、RPCマネージャ732によってサポートされるRPCサービスインターフェースは、サードパーティ販売者によって開発されたアドオンサービスモジュールをサポートするため、またROS602をプログラムすることを簡単にして規模変更を容易にするために標準化および公開され得る。好ましい実施形態のRSIは、最小限の努力で多くのプラットホームのために共通コードを開発し得るように、ほぼ完全にブロック装置のためのDOSおよびUnix装置ドライバモデルに従っている。共通エントリポイント(entry points)の1つの可能なセットの例を、以下の表にリストした。

インタフェースコール	説明
SVC_LOAD	サービスマネージャをロードし、そのステータス(status)をリターンする
SVC_UNLOAD	サービスマネージャをアンロードする
SVC_MOUNT	動的にロードされたサブサービスをマウント(mount)(ロード)し、その状況をリターンする
SVC_UNMOUNT	動的にロードされたサブサービスをアンマウント(unmount)(アンロード)する
SVC_OPEN	マウントされたサブサービスを開く
SVC_CLOSE	マウントされたサブサービスを閉じる
SVC_READ	開いたサブサービスからブロックを読みとる
SVC_WRITE	開いたサブサービスにブロックを書き込む
SVC_IOCTL	サブサービスまたはサービスマネージャを制御する

ロード

好ましい実施形態において、サービス(およびRPCマネージャ732に提示する関連RSI)は、RPC LOADを発行するインストレーションブート処理によって、ブートの間活動化され得る。この処理は、構成ファイルからRPCサービステーブルを読みとり、(カーネルリンク(kernel linked)装置ドライバとは対照的に)ランタイムロード可能(run time loadable)であればサービスモジュールをロードし、次いでサービスのためにLOADエントリポイントをコールする。LOADエントリポイントからの首尾良いリターンは、サービスが適切にロードされ、リクエストを受容する用意があることを示す。

RPC LOADコール例：SVC_LOAD(long service_id)

このLOADインターフェースコールは、権利オペレーティングシステム602初期化の間に、RPCマネージャ732によってコールされる。サービスマネージャが、いずれの動的にロード可能なコンポーネントもロードすること、およびサービスによって必要となる装置およびメモリを初期化することを可能にする。サービスが

ロードされる際のサービス番号は、service_idパラメータとして渡される。好ましい実施形態においては、初期化処理が首尾良く完了した場合にはサービスは０、また何らかのエラーが生じた場合にはエラー番号をリターンする。

マウント

いったんサービスがロードされると、全てのサブサービスに対して完全には機能しないかもしれない。サブサービスによっては（例えば、通信ベースサービス）は、追加の接続の確立を必要とし、またはロードされる追加のモジュールを必要とし得る。サービスが「マウント可能」と規定されれば、RPCマネージャ732は、サブサービスの例を開くのに先だって、リクエストされたサブサービスIDでMOUNTサブサービスエントリポイントをコールする。

RPC MOUNTコール例：

SVC_MOUNT(long service_id, long subservice_id, BYTE' buffer)

このMOUNTインターフェースコールはサービスを命令し、特定のサブサービスを用意する。これは、ネットワーキング、通信、他のシステムサービス、または外部リソースに関係したサービスを含み得る。service_id、およびsubservice_idパラメータは、リクエストされた特定のサービスに固有であり得る。バッファパラメータは、特定サービスに適切な制御ストラクチャを参照するメモリアドレスである。

開く

いったんサービスがロードされ、「マウント」されると、サービスの特定の事例が使用のために「開かれ」得る。サービスの事例を「開く」ことによって、メモリが制御およびステータス情報を格納するようにアロケートし得る。例えば、BSDソケットベースネットワーク接続において、LOADコールが、ソフトウェアおよびプロトコル制御テーブルを初期化し、MOUNTコールがネットワークおよびハードウェアリソースを特定し、そしてOPENが遠隔インストレーションに対してソケットを実際に開く。

安全なデータベースサービスの根底にある商用データベースマネージャ730などサービスによっては、「マウント可能」でないかもしれない。この場合、LOADコ

ールは、データベースマネージャ730と接続し、記録が読み取り可能であることを確実にし得る。OPENコールは、種々のクラスの記録のための内部キャッシュマネージャ746の事例を作成し得る。

RPCOPENコール例：

SVC_OPEN(long service_id、)long subservice_id、BYTE *buffer、int(*receive)(long request_id))

このOPENインターフェースコールは、特定のサブサービスを開くサービスを命令する。service_idおよびsubservice_idパラメータは、リクエストされる特定のサービスに固有であり、バッファパラメータは特定サービスに適切な制御ストラクチャを参照するメモリアドレスである。

任意の受け取りパラメータは、メッセージがそれを検索するサービスに対する用意ができ次第サービスによってコールされる通知コールバック機能のアドレスである。このアドレスへのコールの１つは、受け取られる各入力メッセージに対して作られる。コールする者(caller)が、インターフェースにNULLを渡せば、ソフトウェアは各メッセージに対してコールバックを発生しない。

クローズ、アンマウント、およびアンロード

OPEN、MOUNT、およびLOADコールの反対は、CLOSE、UNMOUNT、およびUNLOADである。これらのインターフェースコールは、アロケートされたリソースをいずれもROS602(例えば、メモリマネージャ680a)に戻す。

RPC CLOSEコール例：SVC_CLOSE(long svc_handle)

このLOADインターフェースコールは、開いたサービス"ハンドル"を閉じる。サービス"ハンドル"は、ユーザが閉じたいと思っているサービスおよびサブサービスを描写する。CLOSEリクエストが首尾良く行われればコールは０をリクエストし(ハンドルは無効となり)、さもなければエラー番号をリターンする。

RPC UNLOADコール例：SVC_UNLOAD(void)

このUNLOADインターフェースコールは、権利オペレーティングシステム602のシャットダウンまたはリソースリアロケーションの間にRPCマネージャ732によってコールされる。開いているどの接続もサービスが閉じ、バッファをフラッシュ

(flush)し、アロケートし得たいずれのオペレーティングシステムリソースも放出することを可能にする。サービスは０をリターンする。

RPC UNMOUNTコール例：SVC_UNMOUNT(long service_id、long subservice_id)

このUNMOUNTインターフェースコールは、特定のサブサービスを非活性化するようにサービスを命令する。service_idおよびsubservice_idパラメータは、リクエストされる特定のサービスに固有であり、SVC_MOUNT()リクエストを使用して予めマウントされていなければならない。コールは、サブサービスに関連した全てのシステムリソースを、そのリターンに先だって放出する。

読み取りおよび書き込み

READおよびWRITEコールは、マウントされ、開かれたサービスへ情報を送り、応答を受け取るための基本的なメカニズムを提供する。例えば、サービスは、RPCリクエストの形で書き込まれたリクエストを有し、その応答がでるとRPCマネージャ732によって読まれ得るようにする。

RPC READコール例：

SVC_READ(long svc_handle、long request_id、BYTE *buffer、long size)

このREADコールは、サービスからメッセージ応答を読みとる。svc_handleおよびrequest_idパラメータは、リクエストを一義的に識別する。リクエストの結果は、ユーザ指定バッファにその限界バイト(size bytes)に達するまで格納される。バッファが小さすぎる場合、メッセージの第１の限界バイトは、バッファに格納され、エラーがリターンされる。

メッセージ応答が、コールする者のバッファに正確にリターンされた場合、機能は０をリターンする。さもなくば、エラーメッセージがリターンされる。

RPC WRITEコール例：

SVC_write(long service_id、long subservice_id、BYTE *buffer、long size、int(*receive)(long request_id))

このWRITEコールは、service_id/subservice_idパラメータペアに特定されたサービスおよびサブサービスにメッセージを書き込む。メッセージはバッファに格納され(そして通常VDE RPCメッセージフォーマットに適合する)、限界バイト

長である。機能は、メッセージのためにリクエストidをリターンする(その送達が受容された場合)さもなくばエラー番号をリターンする。仮に、ユーザが受取りコールバック機能を特定した場合、発生されたメッセージコールバックの代わりにリクエスト特定コールバックルーチンにリクエストに関する全てのメッセージが送られる。

インプット/アウトプット制御

IOCTL(インプット/アウトプット制御)コールは、ロードされたサービスのステータスの照会および制御のためのメカニズムを提供する。各サービスタイプは、特定の汎用IOCTLリクエスト、全ての必要とされるクラスIOCTLリクエスト、およびサービス特定IOCTLリクエストに応答する。

RPC ICTLコール例：ROI_SVC_IOCTL(long service_id、long subservice_id、int command、BYTE* buffer)

このIOCTL機能は、RSIのための汎用化された制御インターフェースを提供する。ユーザは、制御したいservice_idパラメータ、およびsubservice_idパラメータ

を指定する。制御コマンドパラメータ、およびコマンドパラメータが書き込ま/読み取られ得るバッファを指定する。コマンドおよび適切なバッファストラクチャのリストの例を以下に示す。

コマンド	ストラクチャ	説明
GET_INFO	SVC_INFO	サービス/サブサービスについての情報をリターンする
GET_STATS	SVC_STATS	サービス/サブサービスについての現状統計値をリターンする
CLR_STATS	なし	サービス/サブサービスについての統計をクリアする

＊　＊　＊　＊　＊

好ましい実施形態によって提供される包括的なRPCサービスインターフェースを説明してきた。以下の説明は、ROS602によって提供されるサービスの特定の例に関する。

SPE装置ドライバ736

SPE装置ドライバ736は、ROS602とSPE503とのインターフェースを提供する。好ましい実施形態におけるSPE503は、SPU500の境界内でランされるため、この装置ドライバ736の１つの局面は、SPU500ハードウェアとの低レベル通信サービスを提供することである。SPE装置ドライバ736の他の局面は、特にSPE503に、RPCサービスインターフェース(RSI)736aを提供することである(この同じRSIは、HPE装置ドライバ738を介してHPE655と通信するために使用され得る)。

SPE RSI736aおよびドライバ736は、簡潔な機能セットを提供する基本インターフェースポイントのセットを提供することによって、ROS602内(またはROSの外部)のコーリング処理を、SPE503によって提供される細目にわたるサービスから孤立させる。これには、いくつかの利点がある。例えば、外界には共通の機能性を提供するが、詳細な内部ストラクチャおよびアーキテクチャが異なり得る規模

変更されたSPU500のフルライン(full line)が許容される。装置内のメモリ常駐容量、プロセッサ速度、およびSPU500内でサポートされているサービスの数などのSPU500の特性は、特定SPU製造業者によって決定され得、とにかく一方のSPU構成と他方とでは異なり得る。互換性を維持するために、SPE装置ドライバ736およびRSI736aは、サポートし得るSPU500および/またはSPE503の詳細な構成の差異を隠す基本共通RPCインターフェース規格への適合を提供する。

そのような適合性を提供するために、好ましい実施形態におけるSPE RSI736aは、簡単なブロックベース規格に従う。好ましい実施形態において、SPE RSI736aは、ネットワークEthernetカードのパケットインターフェースの後にモデル化され得る。この規格は、好ましい実施形態におけるSPU500のブロックモードインターフェース特性を綿密にモデル化する。

SPE RSI736aは、RPCマネージャ732からのRPCコールが、SPE736によって提供された特定のサービスにアクセスすることを可能にする。これを実現するために、SPE RSI736aは、サービス通知アドレスインターフェースのセットを提供する。これらは、SPE503によって提供される個別のサービスに、外界とのインターフェースを提供する。RPCコールをSPE RSI736aを向け、RPCコール内の対応するサ

ービス認知アドレス：を特定することによって、ROS602内のいかなるコーリング処理もこれらのSPEに提供サービスにアクセスし得る。特定された'サービス認知アドレス：は、SPE503に、SPE内の特定のサービスにRPCコールを内部的にルートさせる。以下は、個別のサービス認知アドレスが提供され得るSPEサービス故障の一例の一覧である：

チャネルサービスマネージャ

認証マネージャ/安全通信マネージャ

安全データベースマネージャ

チャネルサービスマネージャは、主要サービスプロバイダであり、残りのROS602のためのSPE503へのアクセスポイントである。後述されるように、イベント処理はこのサービスによって主に管理される（SPE503の外部における処理の観点から）。認証マネージャ/安全通信マネージャは、ROS602のユーザのためのログイン/ログアウトサービスを提供し、コンポーネントアセンブリ690、VDEオブジェクト300などに関連した（典型的には暗号化、もしくは保護された）通信を管理するための直接サービスを提供し得る。情報表示のリクエスト（例えば、金融予算の残高）は、SPE503内の安全データベースマネージャへの直接サービスリクエストによって提供され得る。認証マネージャ/安全通信マネージャおよび安全データベースマネージャの事例は、たとえ入手可能であったとしても、SPE503内で動作している処理に利用可能な情報および/または能力のサブセットのみを提供し得る。前記されたように、SPEにエンターするほとんどの（場合によっては全てかもしれない）サービスリクエストは、処理のためにチャネルサービスマネージャにルートされる。その詳細が後述されるように、ほとんどの制御ストラクチャおよびイベント処理論理が、チャネルサービスマネージャの管理の下でコンポーネントアセンブリ690を伴う。

SPE503は、この例において、関連SPEドライバ736を介してアクセスされなければならない。一般的に、SPEドライバ736へのコールは、RPCコールに応答してつくられる。この例においては、SPEドライバRSI736aは、SPEドライバ736についての情報を制御または確かめるために向けられるRPCコールを、ドライバコールに

翻訳し得る。SPEドライバRSI736aは、SPEを介してドライバ736とともにSPE503に向けられたRPCコールを渡し得る。

以下の表は、SPE装置ドライバ736の一例を示す：

エントリポイント	説明
SPE_info()	SPEドライバ736(およびSPE503)についてのサマリ情報をリターンする
SPE_initialize_interface()	SPEドライバ736を初期化し、受け取ったパケットのためのデフォルト認知アドレスをセットする
SPE_terminate_interface()	SPEドライバ736を終了し、SPU500およびドライバ736をリセットする
SPE_reset_interface()	SPU500をリセットすることなくドライバ736をリセットする
SPE_get_stats()	認知アドレスおよび/または全ドライバ736のための統計をリターンする
SPE_clear_stats()	特定の認知アドレスおよび/または全ドライバ736の統計をクリアする
SPE_set_notify()	特定サービスIDのための認知アドレスをセットする
SPE_get_notify()	特定サービスIDのための認知アドレスをリターンする
SPE_tx_pkt	(例えば、RPCコールを含む)パケットを処理のためにSPE503に送る

以下に、上記の表に記載される各SPEドライバコールのより詳細な例である。

SPE情報ドライバコールの例：SPE_info(void)

この機能は、SPE装置ドライバ736aを定義するSPE_INFOデータストラクチャにポインターをリターンする。このデータストラクチャは、SPE装置ドライバ736、RSI736a、および/またはSPU500についての特定の情報を提供し得る。SPE_INFOストラクチャの例を以下に示す：

SPE装置ドライバ736のバージョンナンバー/ID
SPE装置ドライバRSI736のバージョンナンバー/ID
SPE装置ドライバ736のネームへのポインター
SPU500のIDネームへのポインター
SPE能力/機能性を示す機能性コード

SPE初期化インターフェースドライバコールの例

SPE_initialize_interface(int(fcn receiver)(void))

set_notify()コールを用いて宛先サービスが置き換え(over-ridden)られない限り、SPE503から受け取った全てのパケットに対して、パラメータによって渡されるレシーバ機能がコールされる。受け取り機能は、ROS602が、RPCマネージャ732とSPE503との間のパケット通信のためのフォーマットを特定することを可能にする。

好ましい実施形態において、この機能は、インターフェースの初期化が成功すれば0をリターンし、失敗すれば非ゼロをリターンする。機能が失敗した場合、失敗の理由を説明するコードを関数値としてリターンする。

SPE終了インターフェースドライバコールの例

SPE_terminate_interface(void)

好ましい実施形態において、この機能は、SPEドライバ736をシャットダウンし、全ての通知アドレスをクリアし、SPEとROS RPCマネージャ732との間の全ての未決着の(outstanding)リクエストを終了する。この機能はまた、全てのリクエストの決着がついた(resolve)後に、SPE503を(例えば、SPU500のウォームリブートによって)リセットする。

ドライバ736の終了は、オペレーティングシステムがシャットダウンを始める時にROS602によって行われる。また、SPEにおける全ての処理が既知の状態(known state)にリセットされなければならないほど、SPE503およびROS602が同期しなくなれば、コールを発行することが必要となる。

SPEリセットインターフェースドライバコールの例：

SPE_reset_interface(void)

この機能は、ドライバ736をリセットし、SPE503とROS RPCマネージャ732との間の全ての未決着のリクエストを終了し、全ての統計カウントをクリアする。この機能は、SPE500をリセットせず、単純にドライバ736を既知の安定状態に復元する。

SPE ゲット(Get)統計 ドライバコールの例：SPE_get_stats(long service_id)

この機能は、一般的に、特定のサービス通知インターフェースまたはSPEドライバ736のために統計をリターンする。この機能は、これらの統計、または(インターフェースが初期化されていないためか、レシーバアドレスが特定されていないためのいずれかの理由によって)統計がなければNULLを含む統計バッファにポインタをリターンする。SPE_STATSストラクチャの一例は、以下の定義を有し得る：

Service id
packets rx
packets tx
bytes rx
bytes tx
errors rx
errors tx
requests tx
req tx completed
req tx cancelled
req rx
req rx completed
req rx cancelled

ユーザがサービスIDを特定した場合、そのサービスによって送られたパケットに関連した統計がリターンされる。ユーザがパラメータとして0を特定した場合、インターフェースのための合計パケット統計がリターンされる。

SPE「クリア統計」ドライバコールの例：

SPE_clear_stats(long sevice_id)

この機能は、特定されたSPE_service_idに関連した統計をクリアする。service_idが特定されなかった場合（すなわち、コールする者が０で渡した場合）、グローバル統計がクリアされる。この機能は、統計が首尾良くクリアされた場合には０をリターンし、エラーが発生した場合にはエラー番号をする。

SPE「セット通知アドレス」ドライバコールの例：

SPE_set_notify(long service_id, int(fcn far receiver)(void))

この機能は、特定のサービスのために、通知アドレス（レシーバ）をセットする。通知アドレスがNULLにセットされた場合、SPE装置ドライバ736は、特定されたサービスへのパケットの通知をデフォルト通知アドレスへ送る。

SPE「ゲット通知アドレス」ドライバコールの例

SPE_get_notify(long service_id)

この機能は、ネームサービスに関連した通知アドレスをリターンし、もしくは特定の通知アドレスが特定されなければNULLをリターンする。

SPE「送りパケット（Send Packet）」ドライバコールの例：

send_pkt(BYTE far buffer, long size, int(far far receive)(void))

この機能は、「長さ」サイズのバッファに格納されたパケットを送る。パケットが首尾良く送られた場合には０を送り、さもなくば失敗に関連したエラーコードを送る。

リディレクタサービスマネージャ684

リディレクタ684は、既存するオペレーティングシステムへの「アドオン」によってROS602が設けられる場合、または先において説明したように、何らかのVDE機能のために「トランスペアレント」オペレーションが望ましい場合に主に使用されるシステム統合ソフトウェアの一部である。１つの実施形態において、カーネル680、通信マネージャ776の一部、ファイルシステム687、およびAPIサービス742の一部は、DOS、Windows、UNIX、Macintosh System、OS9、PSOS、OS/2、または他のオペレーティングシステムプラットホームなどの既存するオペレーティング

システムの一部をなし得る。図12に示すROS602サブシステムの残りは、既存のオペレーティングシステムへの「アドオン」として設けられ得る。いったんこれらのROSサブシステムが供給され、「アドオン」されると、統合された全体が図12に示すROS602を含む。

この種の統合の摘要においては、ROS602は、継続して既存のＯＳカーネル680によってサポートされるが、例えば、仮想メモリマネージャなど追加のアドオン部分を設けることによってその機能の多くを補足（または置換）し得る。

また、この統合摘要においては、既存のAPIサービスと容易に統合するAPIサービス742のアドオン部分が、VDE機能コールをサポートするために設けられる。アドオン部分を統合された既存APIサービスは、VDE機能604へのコール、およびVDE機能以外の機能606へのコールの両方（図11Aを参照）を含むオペレーティングシステムコールの向上したセットをサポートする。APIサービス742のアドオン部分は、RPCマネージャ732によるルーティングのために、VDE機能コールをRPCコールに翻訳し得る。

ROS602は、既存のオペレーティングシステムの提供する標準通信マネージャ776を使用、または容易に統合し得る「アドオン」および/またはその代用品を設け得る。リディレクタ684は、この統合機能を提供し得る。

これは、ROS602を既存のファイルシステム687と統合するという要件を残す。リディレクタ684は、この統合機能を提供する。

この統合摘要において、既存のオペレーティングシステムのファイルシステム687は、補助記憶装置への全てのアクセスのために使用される。しかし、VDEオブジェクト300は、補助記憶装置に外部オブジェクト容器728、ファイルシステム687の形態で、または通信マネージャ776を通して遠隔的にアクセス可能に格納され得る。オブジェクトスイッチ734は、外部オブジェクト容器728にアクセスしたい場合には、オブジェクト容器マネージャ770にリクエストし、オブジェクト容器マネージャ770はリクエストをオブジェクト容器728またはリディレクタ692（これは次いでファイルシステム687内のオブジェクトにアクセスする）にルートする。

一般に、リディレクタ684は、VDEオブジェクト容器728コンテンツを、ファイ

ルシステム687への既存コールへマップする。リディレクタ684は、オブジェクトを既存のＯＳのネームスペースへのマッピングを含む、VDEオブジェクト300についての既存ＯＳレベル情報を提供する。これにより、既存のオペレーティングシステムによって提供される「ノーマル」ファイルシステム687アクセス技術を用いたVDE保護されたコンテンツへのシームレスなアクセスが許可される。

前述された統合摘要において、各既存ターゲットＯＳファイルシステム687は、異なるインターフェース要件を有しており、それにより、リディレクタメカニズム

ム684が「フック」され得る。通常、今日の既製のオペレーティングシステムは、ネットワークベースボリューム、ファイルシステム、および他の装置（例えば、プリンタ、モデムなど）に対するサポートを提供するため、リディレクタ684は、低レベルネットワークおよびファイルアクセス「フック」を使用して、既存のオペレーティングシステムと統合し得る。VDE機能602をサポートするための「アドオン」は、これらの既存のフックを使用して、既存のオペレーティングシステムに統合し得る。

ユーザ通知サービスマネージャ740

ユーザ通知サービスマネージャ740および関連ユーザ通知例外インターフェース（「ポップアップ」）686は、電子機器600のユーザとの通信能力が向上したROS602を提供する。全てのアプリケーション608が、API682を通って渡されるROS602からのメッセージに応答するように設計されうるわけではなく、とにかくアプリケーションがどのような状態にあってもユーザと通信する能力をROS602に与えることが重要または望ましい。ユーザ通知サービスマネージャ740およびインターフェース686は、API682およびアプリケーション608を通してリターンコールを渡す代わりにまたはそれに加えて、直接ユーザと通信するメカニズムをROS602に提供する。これは、例えば、Windowsオペレーティングシステムが、ランしているアプリケーションの「上に」、アプリケーションの状態とは無関係に、ユーザメッセージを「ダイアログボックス」に表示する能力に類似する。

好ましい実施形態におけるユーザ通知686ブロックは、アプリケーションコー

ドとして実施され得る。インターフェース740aの実施は、好ましくは、APIサービスマネージャ724の一部として実施され得る通知サービスマネージャ740の上に形成される。好ましい実施形態における通知サービスマネージャ740は、特定通知を、適切なAPIリターンまたはその他の通路を介して、適切なユーザ処理にディスパッチするために、通知サポートを提供する。このメカニズムによって、通知が、通知メカニズムを特定した処理に単に戻るのではなく、どの承認された処理にもルートされることを可能になる。

APIサービスマネージャ742

好ましい実施形態のAPIサービスマネージャ742は、RPCサービスマネージャ732とのサービスインターフェースとして実施される。全てのユーザAPIリクエストが、この基本インターフェースの上に形成される。APIサービスマネージャ742は、好ましくはランしている各ユーザアプリケーションのためのサービスの事例を提供する。

好ましい実施形態において、APIサービスマネージャ742にサポートされるROS機能へのRPCコールのほとんどが、何らかの追加のパラメータチェックを伴って、サービスコールに直接マップされ得る。このメカニズムは、開発者が、自らの拡張APIライブラリを、機能性を追加または変更して作成することを可能にする。

「アドオン」を既存のオペレーティングシステムと統合することによって、ROS602が形成される前述された摘要においては、APIサービス742コードは、アプリケーションプログラマーの実施決定、および/または電子機器600のタイプによって、共有され得る(例えば、Windows DLLのようなホスト環境なかのレジデント(resident))、またはアプリケーションのコードと直接リンクされ得る。通知サービスマネージャ740は、API682内で実施され得る。これらのコンポーネントは、システムとユーザスペースとの間の遷移(transition)を提供するために、通知サービスコンポーネント686とのインターフェースをとる。

安全データベースサービスマネージャ(「SDSM」)744

安全データベース600を管理するために使用されうる手法は少なくとも２つあ

る：

Ｃ　商用データベースアプローチ；および

Ｃ　サイト記録番号アプローチ。

ＶＤＥサイトが安全データベース６１０に格納された記録の数に基づいて、どちらかの手法が選択され得る。

商用データベースアプローチは、商用データベースを使用して、安全にラップされた記録を安全に商用データベースに格納する。この手法は、安全データベース６１０に格納された記録の数が多い場合に好ましい。この手法により、リソース使用の費用で（ほとんどの商用データベースマネージャが、多くのシステムリソースを用いる）、高速アクセス、効率的な更新、およびホストシステムへの簡単な統合が提供される。

サイト記録数アプローチは、「サイト記録数」（ＳＲＮ）を使用して、システム内の記録を突き止める。この体系は、安全データベース６１０に格納された記録の数が少なく、大幅に経時変化しないと思われる場合に好ましい。この手法により、更新能力が限定された、効率的なリソースの使用が可能になる。ＳＲＮは、アクセスを速くし、性能を向上させるために、類似したデータ記録のグルーピングをさらに許可する。

ＶＤＥ１００は、大幅に規模変更可能なため、異なる電子機器６００によって、多くの手法のなかの１つの手法が示唆され得る。例えば、セットトップ（ｓｅｔ ｔｏｐ）、ＰＤＡ、または他のロウエンド電子機器のような限定された環境において、必要となるリソース（メモリ、およびプロセッサ）の容量を限定する好ましいＳＲＮ体系があり得る。ＶＤＥが、デスクトップコンピュータ、サーバ、および情報交換所などのより能力の高い電子機器６００に配備される場合、リソースが限定されない環境において高い性能を提供するため、商用データベース体系がより望ましい。

２つのアプローチにおけるデータベース記録の差異の１つは、フルＶＤＥ ＩＤまたはＳＲＮを用いて記録が特定されるかどうかという点である。２つの体系間で翻訳するために、ＳＲＮ参照は、それが生じるたびに、ＶＤＥ ＩＤデータベース照会と置換し得る。同様に、インデックスまたは他のアイテムへの照会として使用されるＶＤ

ＥＩＤは、適切なＳＲＮ値と置換され得る。

好ましい実施形態においては、既製のデータベースマネージャ730は、安全なデータベース610を維持するために使用される。ＲＯＳ602は、データベースドライバ750およびデータベースインタフェイス748を通して、商用データベースマネージャ730と相互作用する。ＲＯＳ602と外部サードパーティ販売者のデータベース商用データベースマネージャ730との間にあるデータベースインタフェイス748は、いかなるデータベース販売者もが自身の製品にＶＤＥ承諾（ｃｏｍｐｌｉａｎｔ）データベースドライバ750を実施することを可能にするオープン規格（ｏｐｅｎ ｓｔａｎｄａｒｄ）であり得る。

ＲＯＳ602は、ＶＤＥの提供する安全層が商用データベースストラクチャ「の上」にあるように、それぞれの安全データベース610の記録を暗号化し得る。換言すれば、

ＳＰＥ736は、商用データベースマネージャ730によってサポートされるデータベース記録ストラクチャ内に格納され得る安全記録を大きさおよびフォーマットで書き込み得る。商用データベースマネージャ730は、記録を組織化、格納、および検索するために使用され得る。ある実施形態においては、商用データベースマネージャ730の代わりに、専有および/または新しく作成されたデータベースマネージャを使用することが望ましい。しかし、商用データベースマネージャ730によって、例えば、既存のデータベース管理製品を使用する能力などの何らかの利点が得られる。

安全データベースサービスマネージャ（「ＳＤＳＭ」）744は、安全データベース610内の記録を得て、改変し、格納するために、下層の（ｕｎｄｅｒｌｙｉｎｇ）商用データベースマネージャ730をコールする。好ましい実施形態において、「ＳＤＳＭ」744は、商用データベースマネージャ730のストラクチャ「の上」に層を形成する。例えば、全てのＶＤＥ安全情報は、暗号化された形式で商用データベースマネージャ730に送られる。ＳＤＳＭ744は、キャッシュマネージャ746およびデータベースインタフェース748とともに、記録管理、（キャッシュマネージャ746を使用した）キャッシング、および商用データベースシステム730および/または記録マネージャ（の上）の関係サ

ービスを提供し得る。好ましい実施形態におけるデータベースインターフェース748およびキャッシュマネージャ746は、自身のRSIを提示するのではなく、安全データベースマネージャRSI744aを通してRPCマネージャ732がそれらと通信する。

ネームサービスマネージャ752

ネームサービスマネージャ752は、以下の３つのサブサービスをサポートする：ユーザネーム・サービス、ホストネームサービス、およびサービスネームサービス。ユーザネームサービスは、ユーザネームと、ユーザID番号との間のマッピングおよび探索を提供し、またユーザベースリソースおよび情報安全の他の局面をサポートし得る。ホストネームサービスは、他の処理リソース（および例えば、他のホスト電子機器）のネーム（例えば、アドレス、通信接続/ルーティング情報などの他の情報と）とVDEノードIDとの間にマッピングおよび探索を提供する。サービスネームサービスは、サービスネームと、接続情報（例えば、遠隔的なサービスルーティングおよびコンタクト情報）およびサービスIDなどの他の直接関係のある情報との間のマッピングおよび探索を提供する。

好ましい実施形態におけるネームサービスマネージャ752は、外部サービスルーティング情報を直接外部サービスマネージャに提供し得るように、外部サービスマネージャ772に接続される。ネームサービスマネージャ752はまた、安全データベースマネージャ744に接続され、ネームサービスマネージャ752が、安全データベース610に格納されたネームサービス記録にアクセスすることを許可する。

外部サービスマネージャ772およびサービストランスポート786

外部サービスマネージャ772は、外部サービスプロバイダとのインタフェイスをとるために、プロトコルサポート能力を提供する。外部サービスマネージャ772は、例えば、ネームサービスマネージャ752から外部サービスルーティング情報を得て、通信マネージャ776を通して、特定の外部サービス（例えば、他のVDE電子機器600、金融情報交換所など）とのコンタクトを初期化する。外部サービスマネージャ772は、通信を提供するために必要な通信プロトコルおよび他の情報を供給するサービストランスポート層786を使用する。

外部サービスマネージャ772の重要な使用例がいくつかある。いくつかのVDEオブジェクトにおいては、そのコンテンツの一部あるいは全部が、そのVDEオブジェクトについての何らかの使用権を持っているあるいはそれを取得したいと思っているユーザが操作しているものではない電子機器600のオブジェクト容器728に格納され得る。この場合、外部サービスマネージャ772は、所望のVDEオブジェクト(あるいはそのコンテンツ)が格納されている電子機器600への接続を管理し得る。さらに、ファイルシステム687は、リディレクタ684を用いたVDEオブジェクトへのアクセスを許可するネットワークファイルシステム（例えば、Netware、LANtastic、NFS等）であり得る。オブジェクトスイッチ734もまたこの能力をサポートする。

外部サービスマネージャ772を用いてVDEオブジェクトにアクセスする場合、多数の異なる技術が可能である。例えば、関連ヘッダ、コンテンツタグ、（例えば、ネームサービスマネージャ752を用いた）ホストIDからURLへの変換、およびHTTPを意識したサービストランスポート層786のインスタンスを含めることにより、VDEオブジェクトをワールドワイドウェブプロトコル（HTML、HTTP、およびURL）用にフォーマットすることが可能である。

他の例においては、外部サービスマネージャ772を用いて、遠隔イベント処理サービス、（これらのサービスを提供および位置決定(locate)するための）スマートエージェント実行サービス、公開鍵の証明書サービス、遠隔ネームサービス、ならびに、（RSIを有する等）ROS 602 RPCによってサポートされるか若しくはサービストランスポート層786がサポートするプロトコルの使用によってサポートされる他の遠隔機能を位置決定し(locate)、接続し、そしてそれを利用することができる。

発信管理的オブジェクトマネージャ754

発信管理的オブジェクトマネージャ754は、オブジェクトスイッチ734、オブジェクト容器マネージャ770あるいは他のソースから管理的オブジェクトを受け取り、これを別のVDE電子機器に送信する。発信管理的オブジェクトマネージャ754は、正しいデスティネーションへの発信オブジェクトの送信を管理する。発信管

理的オブジェクトマネージャ754は、ネームサービスマネージャ752からルーティング情報を取得し、通信サービス776を用いてオブジェクトを送信することができる。典型的に、発信管理的オブジェクトマネージャ754は、オブジェクトがいつ首尾良く送信されたか、オブジェクトがいつ送信されるべきか、およびオブジェクトの送信に関する他の情報を反映するレコードを、安全なデータベース610（例えば、発送テーブル444）に（SPE 503と協力して）保持する。

着信管理的オブジェクトマネージャ756

着信管理的オブジェクトマネージャ756は、通信マネージャ776を介して他のVDE電子機器600から管理的オブジェクトを受け取る。着信管理的オブジェクトマネージャ756は、オブジェクト容器マネージャ770、オブジェクトスイッチ734あるいは他のデスティネーションにオブジェクトをルーティングし得る。典型的に、着信管理的オブジェクトマネージャ756は、受信したオブジェクト、受信されることが予想されるオブジェクト、ならびに受信したオブジェクトおよび／または予想されているオブジェクトに関する他の情報を記録するレコードを安全なデータベース610（例えば、受信テーブル446）に（SPE 503と協力して）保持する。

オブジェクト容器マネージャ770

オブジェクト容器マネージャ770は、データベースあるいはファイルマネージャの一形態である。オブジェクト容器マネージャ770は、オブジェクト容器728内、データベース内あるいはファイルシステム687内におけるVDEオブジェクト300の格納を管理する。オブジェクト容器マネージャ770は、例えばVDEオブジェクト300に関連するINFORMATIONメソッドを用いて、（コンテンツの要約、アブストラクト、校閲者の注釈、スケジュール、プロモーショナルマテリアル等の）オブジェクトに関する情報をブラウズおよび／またはサーチする能力をも提供し得る。

オブジェクト提出マネージャ774

好適な実施形態におけるオブジェクト提出マネージャ774は、アプリケーション608とオブジェクトスイッチ734との間のインターフェースを提供するので、ある

面ではAPI 682の一部と考えられ得る。例えば、オブジェクト提出マネージャ774

は、ユーザアプリケーションが新たなVDEオブジェクト300を作成することを可能にし得る。オブジェクト提出マネージャ774は、着信／発信管理的オブジェクトマネージャ756および754がVDEオブジェクト300（管理的オブジェクト）を作成することをも可能にし得る。

図12Aは、電子機器600のユーザと通信することにより新VDEオブジェクト300の生成を助長するためには、オブジェクト提出マネージャ774をどのように用いればよいのかを示す。図12Aは、好適な実施形態において、オブジェクトの生成がオブジェクト定義ステージ1220およびオブジェクト作成ステージ1230の２つのステージで行われ得ることを示している。図12Aに示される２つの異なる「ユーザ入力」の図示（774(1)および774(2)）によってオブジェクト提出マネージャ774の役割が表されている。

オブジェクト提出マネージャ774は、その役割あるいはインスタンスの１つとして、ユーザインターフェース774aを提供する。ユーザインターフェース774aは、作成されるVDEオブジェクト300の特定の特性を指定(specifying)するオブジェクトコンフィギュレーションファイル1240をユーザが作成することを可能にする。例えば、このユーザインターフェース774aは、ユーザがオブジェクトを生成したいと思っていることをユーザが指定することを可能にし、オブジェクトが有するコンテンツをユーザが指定(designate)することを可能にし、また、オブジェクト内に含まれる情報の他の特定の局面（例えば、規則および制御情報、識別情報(identifying information)等）をユーザが指定することを可能にし得る。

好適な実施形態におけるオブジェクト定義タスク1220の一部は、オブジェクトに入れられるコンテンツあるいは他の情報を分析することであり得る。オブジェクト定義ユーザインターフェース774aは、作成されるオブジェクト内に含まれる「コンテンツ」あるいは他の情報を分析することによって、ユーザが指定する「原子的エレメント」としてそのコンテンツを定義若しくは組織化するコールをオブジェクトスイッチ734に対して発行し得る。本明細書中の他の箇所に説明されているように、例えば、この「原子的エレメント」組織は、コンテンツを、ユーザが指定するパラグラフ、ページあるいは他の細区分(subdivisions)に分解し得ると

ともに、明示的（例えば、各「原子的エレメント」間に制御文字を挿入）あるいは暗示的であり得る。オブジェクトスイッチ734は、（例えば、非時間依存ストリームインターフェース762およびリアルタイムストリームインターフェース760によって）静的および動的コンテンツを受け取ることができるとともに、ファイルシステム687内に格納された格納コンテンツあるいは他の情報にアクセスしてこれを検索することができる。

オブジェクト定義1240の結果は、作成されるオブジェクトに関する特定のパラメータを指定するオブジェクトコンフィギュレーションファイル1240であり得る。このようなパラメータには、例えば、マップテーブル、鍵管理仕様（key management specifications）、およびイベントメソッドパラメータが含まれ得る。オブジェクト構築ステージ1230は、オブジェクトコンフィギュレーションファイル1240および新オブジェクト内に含まれる情報あるいはコンテンツを入力とし、それらの入力に基づいてオブジェクトを構築するとともにそのオブジェクトをオブジェクト容器728内に格納し得る。

オブジェクト構築ステージ1230は、オブジェクトコンフィギュレーションファイル1240内の情報を用いてコンテナの組立あるいは改変を行い得る。典型的に、このプロセスにおいては、１つ以上のPERC808、公開ヘッダ、秘密ヘッダを作成し、コンテンツを暗号化し、これらを全て新オブジェクト内（あるいは新オブジェクトに関連するレコードの中の安全なデータベース610内）に格納する一連のイベントがSPE 503に通信される。

オブジェクトコンフィギュレーションファイル1240は、オブジェクトスイッチ734内のコンテナマネージャ764に引き渡され得る。コンテナマネージャ734は、オブジェクトコンフィギュレーションファイル1240と、さらなるユーザ入力とに基づいてオブジェクト300を構築する役割を果たす。ユーザは、別のインスタンス774(2)のオブジェクト提出マネージャ774を介してオブジェクト構築1230とインタラクトし得る。オブジェクト提出マネージャ774によって提供されるこのさらなるユーザインタラクションにおいて、ユーザは、新オブジェクト300に適用あるいは関連付けされるパーミッション（permissions）、規則および／または制御情報を指定し得る。パーミッション、規則および制御情報を指定するためには

、一般に、

先に述べたように、オブジェクト提出マネージャ774および／またはオブジェクトスイッチ734内のコンテナマネージャ764が（例えば、ゲートウェイ734を介して）SPE 503にコールを発行することにより、SPEに、安全なデータベース610から適切な情報を取得させ、適切なデータベース項目を生成させ、そして、そのデータベース項目を安全なデータベース610内に格納させるおよび／またはそのデータベース項目を暗号化されプロテクトされた形式でオブジェクトスイッチに提供させてオブジェクトにこれを組み込む必要が生じ得る。SPE 503が提供する上記情報には、暗号化されたコンテンツあるいは他の情報に加えて、１つ以上のPERC 808、１つ以上のメソッドコア1000'、１つ以上のロードモジュール1100、UDE 1200および／またはMDE 1202等の１つ以上のデータ構造、様々な鍵ブロック、タグ、公開および秘密ヘッダならびにエラーコレクション情報が含まれる。

コンテナマネージャ764は、オブジェクトコンフィギュレーションファイル1240によって指定される新オブジェクトコンテンツあるいは他の情報についてのパラメータに少なくとも部分的に基づいて、SPE 503と協力して、オブジェクトコンテナ302を構築し得る。その後、コンテナマネージャ764は、新オブジェクト内に含まれるべき（SPE 503によって暗号化された）コンテンツあるいは他の情報をコンテナ302内に挿入し得る。コンテナマネージャ764は、適切なパーミッション、規則および／または制御情報をもコンテナ302内に挿入し得る（このパーミッション、規則および／または制御情報は、オブジェクト提出マネージャ774を介したユーザインタラクションによって少なくとも部分的に定義することができるとともに、少なくとも部分的にSPE 503によって処理することによって安全なデータ制御構造を作成することができる）。その後、コンテナマネージャ764は新オブジェクトをオブジェクト容器687に書き込むことができ、ユーザあるいは電子機器は、安全なデータベース610内に適切な情報を入れることによって新オブジェクトを「登録」することができる。

通信サブシステム776

上記のように、通信サブシステム776は、ネットワークマネージャ780およびメ

ールゲートウェイマネージャ782を提供する従来型の通信サービスであり得る。

オ

ブジェクト300および他のVDE情報を外界へ／から自動的にルーティングするためにメールフィルタ784を設けてもよい。通信サブシステム776は、ケーブル、衛星あるいは他の遠距離通信リンクからのリアルタイムコンテンツフィード684をサポートし得る。

安全な処理環境503

図12を参照しながら先に説明したように、好適な実施形態において、電子機器600はそれぞれ、１つ以上のSPE 503および／または１つ以上のHPE 655を含む。これらの安全な処理環境はそれぞれ、安全な方法でタスクを行うためのプロテクト下の実行スペースを提供する。これらの安全な処理環境は、ROS 602から引き渡されたサービス要求を実行(fulfill)することができるとともに、それら自身が、ROS 602内の他のサービスによってまたは他のVDE電子機器600若しくはコンピュータが提供するサービスによって満足されるサービス要求を生成することも可能である。

好適な実施形態において、SPE 503はSPU 500のハードウェア資源によってサポートされる。HPE 655は、汎用プロセッサ資源によってサポートされ得るとともに、セキュリティ／保護用のソフトウェア技術に依存(rely)し得る。従って、HPE 655は、マイクロコンピュータ、ミニコンピュータ、メインフレームコンピュータあるいはスーパーコンピュータプロセッサ等の汎用CPU上で特定のコンポーネントアセンブリ690を組み立てて、それを実行する能力をROS 602に与える。好適な実施形態においては、SPE 503の全体ソフトウェアアーキテクチャはHPE 655のソフトウェアアーキテクチャと同じてあり得る。HPE 655は、SPE 503および関連SPU 500を「エミュレート」し得る。即ち、（ROS 602が、SPU 500内でのみ実行されるべき安全性の高い特定のタスクをHPEに送ることは制限され得るが、）ROS 602からの同一セットのサービス要求をサポートするのに必要なサービスおよび資源をそれぞれが有し得る。

一部の電子機器600コンフィギュレーションは、SPE 503とHPE 655とを両方含

む場合がある。例えば、HPE 655が行い得るタスクはセキュリティ保護をそれ程（あるいは全く）必要としないものであり、SPE 503は高度なセキュリティを必要とす

る全てのタスクを行い得る。多重SPEおよび／またはHPEアレンジメントを用いてシリアルまたは同時処理を提供するこの能力は、さらなる柔軟性を提供するとともに、実用上あるいは費用効果上の理由によりSPU 500内の資源が限られていることによる制限を克服し得る。SPE 503とHPE 655との協力は、特定の用途において、VDE 100が要求する安全な処理をサポートおよび提供するためのより効率的、経費効果的、且つ安全な全体処理環境につながり得る。１つの例として、HPE 655は、リリースされたオブジェクト300「コンテンツ」をユーザが操作することを可能にする全体処理を提供し得るが、安全なオブジェクトにアクセスしてそのオブジェクトから情報を開放するのにはSPE 503が用いられる。

図13は、好適な実施形態の安全な処理環境（SPE）503のソフトウェアアーキテクチャを示す。このアーキテクチャは、好適な実施形態のホスト処理環境（HPE）655にも適用し得る。「プロテクト下の処理環境」（「PPE」）650は、広義には、SPE 503および／またはHPE 655を指し得る。以下、コンテキストによってそうでないことが示される場合を除いて、「PPE 650」、「HPE 655」および「SPE 503」のいずれかに言及すれば、それは、それら全てを指し得る。

図13に示されるように、好適な実施形態において、SPE 503（PPE 650）は以下のサービスマネージャ／重要機能的ブロックを含む。

カーネル／ディスパッチャ552

C　　チャネルサービスマネージャ562

C　　SPE RPCマネージャ550

C　　時間ベースマネージャ554

C　　暗号化／復号化マネージャ556

C　　鍵およびタグマネージャ558

C　　要約サービスマネージャ560

C　　認証マネージャ／サービス通信マネージャ564

C　　乱数値発生器５６５

C　　安全なデータベースマネージャ５６６

C　　その他のサービス５９２

以下、PPE 650の上記重要機能的ブロックのそれぞれを詳細に説明する。

Ｉ．SPEカーネル／ディスパッチャ５５２

カーネル／ディスパッチャ５５２は、SPU 500のハードウェア資源上で動いてこれを管理するオペレーティングシステム「カーネル」を提供する。このオペレーティングシステム「カーネル」５５２は、SPU 500の自立オペレーティングシステムを提供するとともに、（ROSが制御／管理しているSPEおよびHPEのそれぞれにつき１つのOSカーネルを含む複数のOSカーネルを有し得る）ROS 602全体の一部でもある。カーネル／ディスパッチャ５５２は、SPUタスクおよびメモリ管理を提供し、内部SPUハードウェア割込みをサポートし、特定のローレベルサービスを提供し、「DTD」データ構造を管理し、そして、SPUバスインターフェースユニット５３０を管理する。また、カーネル／ディスパッチャ５５２は、SPU 500による実行のためにプログラムを安全な実行スペースにロードすることができるロードモジュール実行マネージャ５６８をも含む。

好適な実施形態においては、カーネル／ディスパッチャ５５２は以下のソフトウエア／機能的構成部材を含み得る。

ロードモジュール実行マネージャ５６８

タスクマネージャ５７６

メモリマネージャ５７８

仮想メモリマネージャ５８０

「ローレベル」サービスマネージャ５８２

内部割込みハンドラー５８４

BIUハンドラー５８６（HPE 655内に存在しない場合もある）

サービス割込みキュー５８８

DTDインタプリタ５９０

好ましくは、カーネル／ディスパッチャ５５２の少なくとも一部が、SPU ROM 532

内にロードされたSPUファームウェア(firmware)内に格納される。SPU ROM 532のメモリマップの一例を図14Aに示す。このメモリマップは、SPU ROM 532aおよび／またはEEPROM 532b内に常駐するカーネル／ディスパッチャ552の様々な構成部材（および図13に示される他のSPEサービス）を示す。図14Bに示すNVRAM 534bのメ

モリマップの例には、タスクマネージャ576およびNVRAMにロードされる他の情報が示されている。

カーネル／ディスパッチャ552によって行われる機能の１つは、ROS RPCマネージャ732からRPCコールを受け取ることである。先に説明したように、ROSカーネルRPCマネージャ732は、RPCコールを、SPEによる処理(action)のために、（SPEデバイスドライバ736およびその関連RSI 736aを介して）SPE 503にルーティングすることができる。SPEカーネル／ディスパッチャ552はこれらのコールを受け取り、そして、それらを処理するか、またはそれらをSPE RPCマネージャ550に引き渡してSPE 503内にルーティングする。SPE 503に基づく処理によって、RPC要求を生成することも可能である。これらの要求の一部は、SPE 503によって内部処理され得る。これらの要求が内部でサービス不可能である場合、これらをSPEカーネル／ディスパッチャ552を介してSPE 503の外部のROS RPCマネージャ732に引き渡して、SPE 503外部のサービスへとルーティングすることが可能である。

Ａ．カーネル／ディスパッチャタスク管理

カーネル／ディスパッチャタスクマネージャ576は、SPE 503（PPE 650）内で実行するタスクをスケジュールおよび監視する。SPE 503は多くの種類のタスクをサポートする。「チャネル」（好適な実施形態におけるコンポーネントアセンブリ690の実行を制御する特別な種類のタスク）は、タスクマネージャ576によってタスクの１種として扱われる。タスクは、実行のためにタスクマネージャ576に提出される。次に、タスクマネージャ576は、そのタスクを実行するために必要なSPE 503／SPU 500資源が利用可能であることを確実にし、そして、SPUマイクロプロセッサ520の手配を整えてタスクを実行する。

カーネル／ディスパッチャ552へのあらゆるコールは、SPE 503の支配権を握っ

て現在実行している１つあるいは複数のタスクを変更する機会をカーネルに与える。従って、好適な実施形態のカーネル／ディスパッチャタスクマネージャ576は、（仮想メモリマネージャ580および／またはメモリマネージャ578に関連して）現在アクティブのタスクの中のいずれかあるいはその全てを実行スペースから「スワップアウト」して、付加的なあるいは異なるタスクを「スワップイン」し得る。

タスクマネージャ576によって管理されるSPEタスク処理は、「単一タスク処理」（一度に１つのタスクのみがアクティブであり得るという意味）あるいは「多重タスク処理」（一度に複数のタスクがアクティブであり得るという意味）のいずれかである。好適な実施形態において、SPE 503は、単一タスク処理あるいは多重タスク処理をサポートし得る。例えば、（サーバデバイス内等の）SPE 503の「ハイエンド」インプリメンテーションは、好ましくは「先制スケジューリング」を用いた多重タスク処理を含む。デスクトップアプリケーションでも数個のタスクを同時に実行することが要求され得るが、デスクトップアプリケーションの場合、比較的シンプルなSPE 503の使用が可能であり得る。セットトップアプリケーションの場合、比較的シンプルなSPE 503のインプリメンテーションを使用して、一度に１タスクのみの実行をサポートすることが可能であり得る。例えば、SPU 500の典型的なセットトップインプリメンテーションは、様々なメソッドが単一タスク処理環境で実行できるようにVDEメソッドの部分集合を組み合わせた単一の「集合（aggregate）」ロードモジュールを用いて簡単な計量、予算作成、および課金を行い得る。しかし、単一タスク処理のみをサポートする実行環境は、比較的複雑な制御構造の使用を制限し得る。このようなSPE 503の単一タスク処理バージョンは、計量および予算作成処理の数および種類における柔軟性と引き替えに、より小さいランタイムRAMサイズ要件を得る。このようなSPE 503のインプリメンテーションもまた、（メモリの制限に依存して）一度に１オブジェクト300の計量に制限され得る。無論、改変や組み合わせによって、「フル多重タスク処理」をサポートするために必要となる付加的なコストを生じずに簡単な単一タスク処理環境以上に能力を向上させることが可能である。

好適な実施形態において、SPE 503における各タスクは、伝統的な多重タスク処理アーキテクチャにおいて「タスク」と考えられ得る「スワッププロック」によって表される。好適な実施形態における「スワッププロック」は、タスクおよびサブタスクを追跡するためにタスクマネージャ576が用いる記帳メカニズム(bookkeeping mechanism)である。スワッププロックは、SPU 500によって提供される安全な実行環境内に「適合する」コードのチャンクおよび関連リファレンスに相当

する。好適な実施形態において、スワッププロックは、共有されているデータエレメント（例えば、ロードモジュール1100およびUDE 1200）、秘密データエレメント（メソッドデータおよびローカルスタック）、ならびにスワップされたプロセス「コンテキスト」情報（例えば、処理を行っていない時にそのプロセスのために設定されたレジスタ）に対するリファレンスのリストを含んでいる。図14Cは、「チャネル」タスク、「制御」タスク、「イベント」タスク、「計量」タスク、「予算」タスク、および「課金」タスク等の複数の異なるタスク／メソッドの「スワッププロック」の数個の例を格納するSPU RAM 532のスナップショットの一例を示す。SPU RAM 532のサイズによっては、「スワッププロック」をRAMからスワップアウトして、その実行が継続できるようになるまで二次記憶装置652内に一時的に格納しておくことが可能である。従って、多重タスク処理モードで動作しているSPE 503は、「スリープ状態」のタスクを１つ以上有し得る。最も単純な形態の場合、これは、現在処理中のアクティブタスクと、「スリープ状態」にあってアクティブ実行スペースから「スワップアウト」されたもう１つのタスク（例えば、その下で上記アクティブタスクが動いている制御タスク）とが存在する。カーネル／ディスパッチャ522はいつでもタスクをスワップアウトし得る。

タスクマネージャ576は、メモリマネージャ578を用いて上記スワップ処理の実行を助長し得る。例えばRAMおよびSPU 500内部の他の記憶装置から適切な情報を読み出して、「スワッププロック」を二次記憶装置652に書き込むことによって、タスクを安全な実行スペースからスワップアウトさせることができる。二次記憶装置652からスワッププロックを読み出して、適切な情報をSPU RAM 532内に書き

込んで戻すことによって、カーネル552はタスクをスワップして安全な実行スペースに戻すことができる。二次記憶装置652は安全ではないので、SPE 503がそのスワップブロックを二次記憶装置に書き込む前に、各スワップブロックを暗号化し且つ(例えば、SPU 500内部でのみ知られている秘密の値で初期化した一方向ハッシュ関数を用いて)暗号学的に封印しなければならない。さらなる実行のためにスワップブロックを安全な実行スペースに戻す前に、SPE 503は、二次記憶装置652から読み出された各スワップブロックの暗号学的封印を復号化および検証(verify)しなければならない。

「スワップブロック」をSPUメモリ内にロードするには、１回以上の「ページング処理」を行うことにより、以前にロードされたスワップブロックに関連するあらゆる「汚いページ」（即ち、SPE 503によって変更されたページ）を、できれば先ずセーブしてから、フラッシングし（flush）、そして、新たなブロックコンテキストのために必要とされるページを全てロードする必要が生じ得る。

好ましくは、カーネル／ディスパッチャ522は、サービス割込みキュー588を用いて「スワップブロック」を管理する。これらのサービス割込みキュー588は、タスク（スワップブロック）およびそのステータス（実行中、「スワップアウト済」、あるいは「スリープ状態」）をカーネル／ディスパッチャ552が追跡することを可能にする。好適な実施形態において、カーネル／ディスパッチャ552は、「スワップブロック」の管理を助長するために、以下のサービス割込みキュー588を維持し得る。

RUNキュー

SWAPキュー

SLEEPキュー

実行スペースに完全にロードされ、マイクロプロセッサ502からの実行サイクルを待っているおよび／または使用しているタスクは、RUNキューにある。（例えば、他のスワップ可能なコンポーネントがロードをされるのを待っているために）「スワップ」アウトされたタスクは、SWAPキューにおいて参照される。（例えば、プロセッササイクル以外の何らかの資源上でブロックされているか、あるいはそ

の時点では必要でないために）「スリープ状態」にあるタスクは、SLEEPキューにおいて参照される。カーネル／ディスパッチャタスクマネージャ576は、例えば、「ラウンドロビン」スケジューリングアルゴリズムに基づいて、RUNキューおよびSWAPキューの間でタスクを移行させ得る。「ラウンドロビン」スケジューリングアルゴリズムは、サービスを待っている次のタスクを選択し、ページインする必要があるもの(pieces)を全てをスワップインし、そして、タスクを実行する。カーネル／ディスパッチャ552タスクマネージャ576は、必要に応じて、SLEEPキューと「アウェイク(awake)」（即ち、RUNあるいはSWAP）キューとの間でタスクを移行させ得る。

多重タスク処理環境において、２つ以上のタスクが同一のデータ構造に書き込みを行おうとした場合、結果的に「デッドロック」あるいは「タスク不足(task starvation)」となる場合がある。「多重糸」タスク処理アレンジメントを用いて「デッドロック」あるいは「タスク不足」を防ぐことができる。好適な実施形態のカーネル／ディスパッチャ552は、「単一糸」あるいは「多重糸」タスク処理をサポートし得る。

単一糸アプリケーションの場合、カーネル／ディスパッチャ552は、個々のデータ構造をそれらがロードされた時の状態で「ロック」する。「ロック」されると、他のどのSPE 503タスクもそれらをロードすることができず、「ブロック」されているため、データ構造が利用可能になるのを待つことになる。現実問題として、単一糸SPE 503を用いると、外部ベンダがロードモジュール1100を作成する能力が制限され得る。なぜなら、外部ベンダがほとんどあるいは全く知らない他のVDEプロセスによる「デッドロック」が起こらないという保証はどこにもないからである。また、部分的に更新されたレコードのコンテキストスワップを行うと、システムの完全性を損ない、未計量使用を可能にし、および／またはデッドロックを引き起こす可能性がある。さらに、このような「ロッキング」は、典型的に時間クリティカルであるプロセスに不確定であり得る遅延をもたらすとともに、SPE 503のスループットを制限し、オーバーヘッド［間接費］を増大させ得る。

この問題を別にしても、ある状況において有用性あるいは能力を制限し得る、SPE 503の単一糸バージョンの作成に関する処理上の重大な問題が他にも存在する。例えば、多重同時実行タスクは、単一糸SPE 503内にあって頻繁に必要とされる同一のデータ構造を用いた処理を行うことができないかもしれない。これは、実効的に、同時タスクの数を１つに制限し得る。さらに、単一糸性(single-threadedness)は、複数の同時タスクに基づいて正確な合計予算を作成する能力を排除し得る。なぜなら、多重同時タスクは、同一の合計予算データ構造を効果的に共有することができないかもしれないからである。単一糸性は、監査処理を他の処理と同時にサポートする能力をも排除し得る。例えば、モニタリングプロセスに関連する予算および計量を監査するために、リアルタイムフィード処理がシャットダウンされなければならないかもしれない。

より実施可能性の高い「単一糸」能力を提供する１つの方法は、カーネル／ディスパッチャ552が仮想ページ処理(handling)アルゴリズムを用いることにより、データ領域への書き込みが行われる際に「汚いページ」を追跡することである。「汚いページ」は、そのスワップブロックに関連するローカルデータの一部としてタスクスワップブロックを用いてスワップインおよびスワップアウトされ得る。タスクが存在する場合、３方向マージアルゴリズム（即ち、オリジナルデータ構造と、現データ構造と、「汚いページ」とをマージして、新たな現データ構造を形成すること）を用いて、「汚いページ」を（SPU 500の他のタスクによって更新されているかもしれない）現データ構造とマージすることが可能である。更新プロセスにおいて、ページが比較およびスワップされる際にデータ構造はロックされ得る。この仮想ページング解決法は、一部のアプリケーションにおいては単一糸を可能にする方法として実行可能であり得るが、このような単一糸インプリメンテーションの使用は、先に述べたベンダ制限によって、専用ハードウェアに限定され得る場合がある。多重ユーザをサポートするあらゆるインプリメンテーション（例えば、「スマートホーム」セットトップ、多くのデスクトップおよび特定のPDAアプリケーション等）は、特定の状況において単一糸デバイスの制限に直面し得る。

フル「多重糸」データ構造書込み能力を使用する際にこれらの制限が許容不可能であることが好ましい。例えば、データベースベンダが用いる種類のある種の「２フェーズコミット」処理を用いて、プロセス間でのデータ構造の共有を可能にすることができる。この「２フェーズコミット」プロセスを実現するために、各スワップブロックは、変更された情報の格納に用いられる付加的なメモリブロックのページアドレスを有し得る。変更ページは、SPEプロセスによって書き込まれたデータエレメントの１つのローカルコピーである。好適な実施形態において、特定のデータ構造に関連付けられた変更されたページリファレンスは、スワップブロックにローカルに格納される。

例えば、SPE 503は、２（変更ページ）／データ構造をサポートし得る。スワップブロック構造のサイズを変更して、更新アルゴリズムが変更ページの全てを処理できるようにすることによって、この制限は容易に改変可能である。変更され

たページを参照するスワップブロックが破棄されようとしているときに、上記コミットプロセスを呼び出すことができる。コミットプロセスは、初めにロードされたオリジナルデータエレメント（例えば、UDE_0）、現データエレメント（例えば、UDE_1）、および変更されたページについて、これらをマージして新たなデータエレメントのコピー（例えば、UDE_{1-1}）を作成する。DTDインタプリタ590によって、そのデータエレメントのDTDを用いて、差を求めることができる。他にそれを参照するスワップブロックがなければ、オリジナルデータエレメントは破棄される（例えば、そのDTD使用カウントによって決定）。

Ｂ．カーネル／ディスパッチャメモリ管理

好適な実施形態のメモリマネージャ578および仮想メモリマネージャ580は、好適な実施形態におけるSPU 500内のROM 532およびRAM 534メモリを管理する。仮想メモリマネージャ580は、フル「仮想」メモリシステムを提供することによって、SPE安全実行スペースにおいて利用可能な「仮想」RAMの容量を、SPU 500によって提供される物理的RAM 534aの容量以上に大きくする。メモリマネージャ578は、安全な実行スペース内のメモリを管理するものであり、メモリのアクセス

、割当および割当解除を制御する。SPU MMU 540が存在する場合、SPU MMU 540は、好適な実施形態における仮想メモリマネージャ580およびメモリマネージャ578をサポートする。一部のSPU 500の「最小」コンフィギュレーションにおいては、仮想メモリ能力が全くなく、メモリ管理機能が全てメモリマネージャ578によって処理される場合がある。メモリ管理を利用して、SPE 503によって提供されるセキュリティの実施を助長することも可能である。例えば、一部のクラスのSPU 500においては、カーネルメモリマネージャ578がハードウェアメモリ管理ユニット(MMU)540を用いて、SPU 500内におけるページレベル保護を提供することができる。このようなハードウェアベースのメモリ管理システムは、不正な(rogue)ロードモジュールによる侵犯からVDEコンポーネントアセンブリ690を保護する効果的なメカニズムを提供する。

さらに、少なくとも部分的にはハードウェアベースMMU 540に基づいて動作するメモリマネージャ578が提供するメモリ管理は、多重保護ドメイン(multiple pro

tection domains)を提供するメモリアーキテクチャを安全に実現および実施し得る。このようなアーキテクチャにおいては、メモリが複数のドメインに分割される。この複数のドメインは、互いに大きく隔てられており、メモリマネージャ578の制御下で特定のメモリ領域のみを共有している。実行プロセスはそのドメインの外部にあるメモリにはアクセスできず、他のプロセスとの通信は、SPU 500内の特権的(privileged)カーネル／ディスパッチャソフトウェア552によって提供および仲介されるサービスによってしか行うことができない。SPU 500内で実行するソフトウェアベースのどんなプロセスによっても改変不可能なMMU 540内のハードウェアによって少なくとも部分的に実施される場合、このようなアーキテクチャはより安全である。

好適な実施形態においては、ROM 532内で実施されるサービスへのアクセスならびにNVRAM 534bおよびRTC 528等の物理的資源へのアクセスは、特権的カーネル／ディスパッチャソフトウェア552とMMU 540内のハードウェアとの組み合わせによって仲介される。クリティカルシステムコンポーネントルーチン(例えば、

RTC 528）を保護するために、ROM 532およびRTC 528要求には特権が与えられる。

メモリマネージャ578は、メモリの割当および割当解除を行い、プロセス間でのメモリ資源の共有を監督し（supervising）、メモリのアクセス／使用制限を実施する役割を果たす。典型的に、SPEカーネル／ディスパッチャメモリマネージャ578は、全てのメモリを初期的にカーネル552に割り当て、ページが特定のプロセスによってロードされるときに、そのページへのプロセスレベルのアクセスのみを許可するように構成され得る。SPE処理システムコンフィギュレーションの１つの例においては、メモリマネージャ578は、単純化された割当メカニズムを用いてメモリの割当を行う。SPE 503内でアクセス可能な各メモリページのリストは、例えばビットマップ割当ベクトルを用いて表され得る。１つのメモリブロックにおいて、一群の連続するメモリページは、ある特定のページ番号から始まり得る。ブロックのサイズは、そのブロックが占めるメモリページの数によって計られる。メモリの割当は、割当ベクトル内に適切なビットをセット／クリアすることによって記録され得る。

メモリ管理機能を助長するために、「ドープベクトル」がメモリブロックの前に付加され得る。「ドープベクトル」は、メモリマネージャ578がそのメモリブロックを管理することを可能にする情報を有し得る。最も単純な形態の場合、メモリブロックは、そのブロックの実際のメモリ領域の手前の「ドープベクトル」として構成され得る。この「ドープベクトル」は、ブロック番号と、データエレメントのダイナミックページングのサポートと、メモリの上書きを検出するためのマーカとを含み得る。メモリマネージャ578は、そのブロック番号によってメモリブロックを追跡して、使用前にブロック番号をアドレスに変換することができる。メモリ領域への全アクセスは、ブロックメモリから物理的アドレスへの変換を行う際に、「ドープベクトル」のサイズ分だけ自動的にオフセットされ得る。また、「ドープベクトル」は、仮想メモリの管理を助長するために仮想メモリマネージャ580によって使用され得る。

好適な実施形態において、メモリマネージャ578によって行われるROM 532メモ

リ管理タスクは比較的単純である。ROM 532ページを全て、「読出し専用」および「ページング不可」としてフラッグ付けすることができる。EEPROM 532Bメモリ管理は、これよりも若干複雑であり得る。なぜなら、各EEPROMページの「バーンカウント」を保持する必要があるかもしれないからである。この種のメモリにおける限られた書込み可能寿命を長持ちさせるために、あらゆる非制御の書込みからSPU EEPROM 532Bをプロテクトすることが必要であり得る。さらに、EEPROMページと、メモリ管理アドレスページとが同一サイズではない場合がある。

好ましくは、SPU NVRAM 534bは、アクセスの制限が少ないバッテリ付きRAMである。メモリマネージャ578は、NVRAM 534b内に配置されていなければならない制御構造が「ゴミ回収」プロセスの間に再配置されないことを確実にすることができる。上記のように、メモリマネージャ578（および、存在する場合、MMU 540）は、NVRAM 534bおよびRAM 534aをページレベルで保護し、他のプロセスによる不正改変を防ぐことができる。

仮想メモリマネージャ580は、SPU外部メモリとSPU内部RAM 534aとの間でのプログラムおよびデータのページングを行う。データ構造および実行可能プロセスは、あらゆるSPU 500内部メモリの限界を越える可能性が高い。例えば、PERC 808および他の基本制御構造はかなり大きく、「ビットマップ計量」は非常に大きい、あ

るいは非常に大きくなる可能性がある。これについては、最終的に２通りの対処法があり得る。

(1) ロードモジュール1100を細分化する

(2) 仮想ページングをサポートする

多くの場合ロードモジュールは別々のコンポーネントに分割され、実行するためにロードする必要があるのはその部分集合のみであるので、ロードモジュール1100は「細分化」可能である。この例において、ロードモジュール1100はページング可能且つ実行可能な最小エレメントである。このようなロードモジュール1100は、別々のコンポーネント（例えば、実行可能なコードおよび複数のデータ記述ブロック）に分割可能であり、単純なロードモジュールを実行するためにロー

ドする必要があるのはその中の１つだけである。この構成によれば、ロードモジュール1100によって初めに実行可能なコードのみをロードしておいて、要求(demand)に応じて他のシステムページ内にデータ記述ブロックをロードすることが可能になる，大きすぎてSPU 500内には適合しない実行可能セクションを有するロードモジュール1100の多くを、２つ以上のより小さい単独ロードモジュールに再構築することができる。明示的なロードモジュールリファレンスを用いれば、大きいロードモジュールを、「連鎖した」複数のロードモジュールにマニュアル「分割」することができる。

「要求ページング(demand paging)」を用いて上記制限を一部緩和することができるが、好適な実施形態においては、仮想ページングを用いて大きなデータ構造および実行可能物を管理している。仮想メモリマネージャ580は、情報（例えば、実行可能コードおよび／またはデータ構造）を、SPU RAM 534aに／から「スワップ」イン／アウトするとともに、他の関連仮想メモリ管理サービスを提供し、これにより、フル仮想メモリ管理能力を実現している。仮想メモリ管理は、資源が限られたSPU 500コンフィギュレーションによる大型および／または多重タスクの実行を可能にする上で重要であり得る。

Ｃ．SPEロードモジュール実行マネージャ568

SPE（HPE）ロードモジュール実行マネージャ（「LMEM」）568は、メモリマネージャ578によって管理されるメモリ内に実行可能物をロードして、それらを実行する。LMEM 568は、プロテクト下の実行環境内に現在ロードされているロードモジュールを追跡するメカニズムを提供する。LMEM 568は、SPE 503内に格納されていてそれ故にSPE 503が常時利用可能な基本ロードモジュールおよびコードフラグメントへのアクセスをも提供する。LMEM 568は、例えば、他のロードモジュールを実行しようとするロードモジュール1100によってコールされ得る。

好適な実施形態においては、ロードモジュール実行マネージャ568は、ロードモジュールエグゼキュータ（「プログラムローダ」）570と、１つ以上の内部ロードモジュール572と、ライブラリルーチン574とを有する。ロードモジュールエグゼキュータ570は、（例えば、メモリマネージャ578からメモリ割当を受け取った

後、)実行可能物をメモリ内にロードしてこれを実行する。内部ロードモジュールライブラリ572は、１セットの一般的に使用される基本ロードモジュール1100(例えば、ROM 532あるいはNVRAM 534b内に格納されている)を提供し得る。ライブラリルーチン574は、SPE 503によって実行される１セットの一般的に使用されるフラグメント／ルーチン（例えば、ブートストラップルーチン）を提供し得る。

ライブラリルーチン574は、標準的な１セットのライブラリ機能をROM 532内に提供し得る。標準的な上記ライブラリ機能のリストならびにその入口点(entry points)およびパラメータを使用することが可能である。ロードモジュール1100は、（例えば、その目的のために用意された割込みを用いて）これらのルーチンをコールし得る。広く使用されるコードを中央に移動してコード再利用の度合いを向上することによって、ライブラリコールはロードモジュールのサイズを低減し得る。好ましくは、SPE 503が使用するロードモジュール1100は全て、利用可能なロードモジュールのリストを維持およびスキャンするとともに適切なロードモジュールを選択して実行するロードモジュール実行マネージャ568によって参照される。SPE 503内にロードモジュールが存在しなければタスクは「スリープ状態(slept)」になり、LMEM 568は、ロードモジュール1100を二次記憶装置562からロードすることを要求し得る。この要求は、安全なデータベースマネージャ566にロードモジュールおよび関連データ構造を検索させるRPCコール、および、メモリマネージャ578によって割り当てられたメモリへのロードモジュールの格納前に、暗号化

／復号化マネージャ556にそのロードモジュールを復号化させるコールの形態であり得る。

もう少し詳細に述べると、好適な実施形態では、所望のロードモジュール1100の名前（例えば、VDE ID）をロードモジュール実行マネージャ568に渡すことによって、ロードモジュール1100が実行される。LMEM 568は先ず、「メモリ内」および「ビルトイン」ロードモジュール572のリストをサーチする。もし所望のロードモジュール1100をリスト内に見つけることができなかった場合、LMEM 568はRPC要求を発行して安全なデータベース610からのコピーを要求する。このRPC要

求は、図12に示されるROS安全データベースマネージャ744によって処理され得る。その後、ロードモジュール実行マネージャ568は、メモリマネージャ578に、ロードモジュール1100格納用のメモリページを割り当てることを要求し得る。ロードモジュール実行マネージャ568は、そのメモリページ内にロードモジュールをコピーし、暗号化／復号化マネージャ556ならびに鍵およびタグマネージャ558による復号化およびセキュリティチェックのためにそのページをキューイングし得る。ページの復号化およびチェックが終わると、ロードモジュール実行マネージャ568は、有効性検査タグをチェックし、ページインされたモジュールのリストにそのロードモジュールを挿入し、そして、ページアドレスを発信者に返す。その後、発信者は、ロードモジュール1100に直接コールするか、あるいはロードモジュール実行モジュール570がそのコールを行うことを許可することができる。

図15aは、チャネルヘッダ596およびチャネル詳細レコード594(1)、594(2)、...594(N)を含んでいるチャネル594の可能なフォーマットの詳細な例を示す。チャネルヘッダ596は、チャネルIDフィールド597(1)と、ユーザIDフィールド597(2)と、オブジェクトIDフィールド597(3)と、「権利」（即ち、PERC 808および／または「ユーザ権利テーブル」464において参照されるメソッドによってサポートされるイベントの収集物（collection））に対するリファレンスあるいは他の識別子(identification)を有するフィールド597(4)と、イベントキュー597(5)と、チャネル詳細レコード（「CDR」）で特定のイベントコードを相互参照する１つ以上のフィールド598とを有し得る。チャネルヘッダ596は、単数あるいは複数の関連コンポーネントアセンブリ690内のエレメントのアドレッシングを可能にする「ジャン

プ」あるいは参照テーブル599をも含み得る。CDR 594(1)、...594(N)は、各々、チャネル594が応答し得る特定のイベント（イベントコード）に対応し得る。好適な実施形態において、これらのCDRは、各メソッドコア1000N（あるいはそのフラグメント）と、ロードモジュール1100と、対応するイベントを処理するために必要なデータ構造（例えば、URT、UDE 1200および／またはMDE 1202）とを、明示的におよび／または参照として有し得る。好適な実施形態においては、１つ以上

のCDR（例えば、594(1)）が、制御メソッドおよびデータ構造としてのURT464を参照し得る。

図15bは、好適な実施形態において、チャネル594を「開く」ためにSPE 503によって行われるプログラム制御ステップの一例を示す。好適な実施形態において、チャネル594は、特定のVDEオブジェクト300、特定の承認されたユーザ、および特定の「権利」（即ち、イベントの種類）のイベント処理を行う。これらの3つのパラメータは、SPE 503に渡され得る。「ブートストラップ」ルーチンにおいてローレベルサービス582によって構築される「チャネル０」内で実行するSPEカーネル／ディスパッチャ552の一部は、SPE 503の処理資源によってサポートされる利用可能なチャネルを割り当てて（ブロック1125）、初期的に「オープンチャネル」イベントに応答し得る。その後、この「チャネル０」「オープンチャネル」タスクは、安全なデータベースマネージャ566に、チャネル594に関連付けられる１つ以上のコンポーネントアセンブリ690を構築するための「ブループリント」を取得させる一連の要求を発行し得る（ブロック1127）。好適な実施形態において、「ブループリント」は、PERC 808および／またはURT464を包含し得る。「オープンチャネル」ルーチンに引き渡された「オブジェクト、ユーザ、権利」パラメータを用いて、オブジェクト登録テーブル460レコードと、ユーザ／オブジェクトテーブル462レコードと、URT464レコードと、PERC 808レコードとを互いに「連鎖」させることによって、ブループリントを得ることができる。好ましくは、この「オープンチャネル」タスクが鍵およびタグマネージャ558にコールして、上記の様々なレコードに関連するタグについて有効性検査および関連付けを行い、これにより、それらのタグが本物であり且つ符合することを確実にする。次に、好適な実施形態のプロセスは、適切な情報をチャネルヘッダ596に書き込み得る（ブロック112

9）。このような情報は、例えば、ユーザID、オブジェクトID、およびチャネルが処理するであろう「権利」に対するリファレンス等を含み得る。好適な実施形態のプロセスは次に、「ブループリント」を用いて、適切な「制御メソッド」に（例えば、安全なデータベース566および／またはロードモジュール実行マネージ

ャライブラリ568から）アクセスし得る（ブロック1131）。この制御メソッドは、チャネル594内の他の全てのメソッド1000の実行を実効的に監督するために用いられ得るものである。プロセスは次に、制御メソッドを上記チャネルに「結合させ(bind)」得る（ブロック1133）。このステップは、URT464からの情報を上記制御メソッドのデータ構造としてチャネル内に結合させることを含み得る。次にプロセスは、チャネル594内に「初期化」イベントを引き渡すことができる（ブロック1135）。この「初期化」イベントは、チャネルサービスマネージャ562（作成されたチャネルによって実行されたサービスを要求するオリジナルのコールを発行したプロセス）によって作成され得る。あるいは、チャネルに結合されたばかりの上記制御メソッド自身が、実効的にそれ自身に渡される初期化イベントを生成し得る。

この「初期化」イベントに応答して、上記制御メソッドは「初期化」イベント以外のさらなるイベントを処理するために用いられるチャネル詳細レコード594(1)、...594(N)を構築し得る。チャネル「内」で実行する制御メソッドは、ステップ1127でアクセスした「ブループリント」に基づいて関連コンポーネントアセンブリ690を構築する必要がある様々なコンポーネントにアクセスし得る（ブロック1137）。メソッドコア1000Nを特定する関連チャネル詳細レコード、ロードモジュール1100、および、イベントに応答するために必要な関連データ構造（例えば、UDE 1200および／またはMDE 1202）を構築することによって、上記コンポーネントが各々チャネル594に結合される（ブロック1139）。チャネル詳細レコードの数は、「ブループリント」（即ち、URT464）によって特定される「権利」がサービスし得るイベントの数に依存する。このプロセスの間、制御メソッドは「スワップブロック」を構築し、これにより実効的に、要求されるタスクを全てセットアップするとともに必要なメモリの割当をカーネル562から取得する。上記制御メソッドは、必要に応じて、安全なデータベースマネージャ566に安全なデータベース

610から必要なコンポーネントを検索させるコールを発行し、暗号化／復号化マネージャ556に検索暗号情報を復号化させるコールを発行し、そして、検索コン

ポーネントが全て有効であることを鍵およびタグマネージャ558に確認させるコールを発行する。このように構築された様々なコンポーネントアセンブリ690のそれぞれは、チャネル詳細レコード594(1)、...594(N)によって参照される適切なスワップブロックを構築することによって、チャネルヘッダイベントコード／ポインタレコード598を介してチャネルに「結合される」。このプロセスが完了した時、チャネル594は完全に構築され、さらなるイベントに応答できるようになっている。最終ステップとして、図15bのプロセスは、それが望まれる場合、「初期化」イベントタスクの割当解除を行って資源を開放(free up)し得る。

このようにしてチャネル594が構築されると、チャネル594は到達するイベントに応答する。チャネルサービスマネージャ562は、チャネル594にイベントをディスパッチする役割を果たす。（例えば、RPCコールによって）新たなイベントが到達する度に、チャネルサービスマネージャ562はイベントを検査(examines)して、そのイベントを処理できるチャネルが既に存在するかどうかを判定する。チャネルが存在する場合、チャネルサービスマネージャ562はそのイベントをそのチャネルに引き渡す。イベントを処理するためには、チャネル詳細レコードによってアクティブタスクであるとされる特定の「スワップ可能ブロック」をタスクマネージャ576によって「スワップイン」する必要が生じ得る。このようにして、図15bに示されるチャネルオープンプロセスの間に形成された実行可能コンポーネントアセンブリ690がアクティブ安全実行スペースに入れられ、そして、受信したイベントコードに応答して、アクティベートされた特定のコンポーネントアセンブリが選択される。その後、アクティベートされたタスクは、イベントに応答して所望の機能を行う。

あるチャネルを破棄(destroy)する際には、チャネル詳細レコードによって定義される様々なスワップブロックが破棄されるとともにチャネルヘッダ596内の識別情報が消去され(wiped clean)、これにより、そのチャネルが「チャネル０」「オープンチャネル」タスクによって再割当可能になる。

Ｄ．SPE割込みハンドラ584

図13に示されるように、カーネル／ディスパッチャ552は内部割込みハンドラ5

84をも提供する。これらは、SPU 500の資源の管理を助長する。好ましくは、全ての重要なコンポーネントについて、SPU 500は「割込み」あるいは「ポーリング」モードで実行する。ポーリングモードにおいて、カーネル／ディスパッチャ552は、SPU 500内のセクション／回路を各々ポーリングし、それらに対する割込みをエミュレートすることができる。好適な実施形態において、好ましくは、以下の割込みがSPU 500によってサポートされる。

C　　RTC 528の「チック」

C　　バスインターフェース530からの割込み

C　　電源異常割込み

C　　ウォッチドッグタイマ割込み

C　　暗号化／復号化エンジン522からの割込み

C　　メモリ割込み（例えば、MMU 540から）

割込みが発生すると、マイクロプロセッサ520内の割込みコントローラは、マイクロプロセッサに適切な割込みハンドラーの実行を開始させ得る。割込みハンドラーは、カーネル／ディスパッチャ552によって提供される1つのソフトウェア／ファームウェアであり、割込みが発生した際にマイクロプロセッサ520が特定の機能を行うことを可能にする。異なる割込み源によって異なる割込みハンドラーが効果的に実行され得るように、割込みは「ベクトル化」され得る。

「タイマチック(timer tick)」割込みは、リアルタイムRTC 528が「拍動する(pulses)」際に発生する。タイマチック割込みをタイマチック割込みハンドラーによって処理することにより、内部デバイスデータ／時間を算出するとともにチャネル処理用のタイマイベントを生成する。

バスインターフェースユニット530は、一連の割込みを発生し得る。好適な実施形態においては、USARTを手本にしたバスインターフェース530が、様々な状態(例えば、「受信バッファ満杯(receive buffer full)」、「送信用バッファ空」、および「ステータスワード変更(change)」)に対して割込みを発生する。カーネル／ディスパッチャ552は、送信キューからの次のキャラクタをバスインターフェー

ス530に送ることによって、送信用バッファ空割込みをサービスする。カーネル／ディスパッチャ割込みハンドラー584は、あるキャラクタを読み込み、それを現バッファに添付し、そして、バスインターフェース530のサービスエンジンの状態に基づいてバッファを処理することによって、受信バッファ満杯割込みをサービスし得る。好ましくは、カーネル／ディスパッチャ552は、ステータスワード変更割込みを処理するとともに、これに従って適切な送信／受信バッファをアドレスする。

SPU 500は、緊急の電力異常状態を検出すると、電源異常割込みを発生する。これには、情報の損失を防ぐために、迅速な対応(action)が要求され得る。例えば、好適な実施形態において、電力異常割込みは、新しく書き込まれた全ての情報（即ち、「汚いページ」）を不揮発性のNVRAM 534b内に移動させ、全てのスワップブロックを「スワップアウト済」とマークし、そして、適切な電力異常フラッグを設定し、これにより、リカバリ処理を容易にする。その後、カーネル／ディスパッチャ552は、データがクリアされるか電源が完全に取り除かれるまでの間、ステータスワード内の「電力異常ビット」を定期的にポーリングし得る。

この例におけるSPU 500は、ウォッチドッグタイマ割込みを定期的に発生する従来型のウォッチドッグタイマを有する。ウォッチドッグタイマ割込みハンドラーは内部デバイスチェックを行って、不正改変が起こっていないことを確認する。ウォッチドッグタイマの内部クロックとRTC 528とを比較することにより、SPU 500が一時停止あるいはプローピングされていないことを確認するとともに、SPU 500の動作に関する他の内部チェックを行って不正改変を検出する。

１ブロックのデータの処理が完了すると、暗号化／復号化エンジン522は割込みを発生する。カーネル割込みハンドラー584は、暗号化あるいは復号化されているブロックの処理ステータスを調節し、そのブロックを次の処理ステージに引き渡す。その後、暗号化サービスを行うことがスケジュールされている次のフ鎖ックは、その鍵を暗号化／復号化エンジン522内に移動させるとともに、次の暗号化プロセスを開始する。

あるタスクがそれに割り当てられた(assigned)領域外のメモリにアクセスしようとした時に、メモリ管理ユニット540割込みが発生する。メモリ管理割込みハ

ン

ドラーは、その要求をトラップして、（例えば、メモリマネージャ578および／または仮想メモリマネージャ580への制御の移行（transfer）を開始することによって）必要な対応をとる。一般には、そのタスクが失敗（failed）するか、ページフォールトイクセプションが生成されるか、あるいは適切な仮想メモリページがページインされる。

Ｅ．カーネル／ディスパッチャローレベルサービス582

好適な実施形態におけるローレベルサービス582は、「ローレベル」機能を提供する。好適な実施形態において、これらの機能には、例えば、電源投入時の初期化、デバイスPOST、および失敗リカバリルーチンが含まれ得る。好適な実施形態において、ローレベルサービス582は、（それら自身によって、あるいは、認証マネージャ／サービス通信マネージャ564との組み合わせによって）ダウンロード応答チャレンジおよび認証通信プロトコルをも提供し得るとともに、（単独で、あるいは、メモリマネージャ578および／または仮想メモリマネージャ580との組み合わせで）EEPROMおよびFLASHメモリ等のSPU 500メモリ装置の特定のローレベル管理を提供し得る。

Ｆ．カーネル／ディスパッチャBIUハンドラー586

好適な実施形態において、BIUハンドラー586は、（存在する場合）バスインターフェースユニット530を管理する。BIUハンドラー586は、例えば、BIU530の読込みおよび書込みバッファを維持し、BIUスタートアップ初期化等を提供し得る。

Ｇ．カーネル／ディスパッチャDTDインタプリタ590

好適な実施形態において、DTDインタプリタ590は、データフォーマットに関する問題を処理する。例えば、DTDインタプリタ590は、DTD内に含まれるフォーマッティング命令に基づいてUDE 1200等のデータ構造を自動的に開き得る。

上記のSPEカーネル／ディスパッチャ552は、SPE 503によって提供される他の全てのサービスをサポートする。他のサービスについて以下に説明する。

II. SPUチャネルサービスマネージャ562

好適な実施形態において、「チャネル」はSPE 503（HPE 655）の基本タスク処理メカニズムである。ROS 602は、「メソッド」のためのイベント駆動型インターフェースを提供する。「チャネル」は、コンポーネントアセンブリ690がイベントをサービスすることを可能にする。「チャネル」は、「イベント」を、SPE 503（HPE 655）によってサポートされるサービスから、それらのイベントを処理するために指定された様々なメソッドおよびロードモジュールに引き渡すための導管（conduit）であるとともに、コンポーネントアセンブリ690の組立およびコンポーネントアセンブリ間のインタラクションをサポートする。より具体的には、チャネルマネージャ593によって維持されるデータ構造の１つである「チャネル」594は、１つ以上のロードモジュール1100とデータ構造（例えば、UDE 1200および／またはMDE 1202）とを１つのコンポーネントアセンブリ690に「結合する」する。チャネルサービスマネージャ562はロードモジュール実行マネージャ569に、実行のためにコンポーネントアセンブリ690をロードさせるとともに、コンポーネントアセンブリ690によるレスポンスのためにチャネル594へとイベントを引き渡すものでもあり得る。好適な実施形態において、イベント処理は、チャネルサービスマネージャ562へのメッセージとして扱われる。

図15は、好適な実施形態のチャネルサービスマネージャ562が「チャネル」594をどのようにして構築するのかを示すとともに、チャネルとコンポーネントアセンブリ690との関係を示す図である。簡潔に述べれば、SPEチャネルマネージャ562は、「チャネル」594およびこれに関連付けられた「チャネルヘッダ」596を確立する。チャネル594およびそのヘッダ596は、１つ以上のコンポーネントアセンブリ690のエレメントを「結合」あるいは参照するデータ構造を含んでいる。従って、好適な実施形態において、チャネル594は、図11Eに示されるエレメントをよせ集めてあるいは組み立てて、イベント処理に使用され得るコンポーネントアセンブリ690にするメカニズムである。

チャネル594は、イベントの発生に応答してチャネルサービスマネージャ562によってセットアップされる。チャネルが作成されると、チャネルサービスマネージャ562は、チャネル594に基づいてロードモジュール実行マネージャ568へ機能

コ

ールを発行し得る。ロードモジュール実行マネージャ568は、チャネル594によって参照されるロードモジュール1100をロードし、カーネル／ディスパッチャタスクマネージャ576による実行サービスを要求する。カーネル／ディスパッチャ552は、そのイベント処理要求を１つのタスクとして扱い、チャネルによって参照されるロードモジュール1100内のコードを実行することによってこれを実行する。

チャネルサービスマネージャ562には、そのイベントの識別子（例えば、「イベントコード」）が引き渡され得る。チャネルサービスマネージャ562は、チャネルサービスマネージャがアセンブルするコンポーネントアセンブリ690の一部である１つ以上のメソッドコア1000'を分解する（parses）。チャネルサービスマネージャ562は、この分解処理を行うことにより、その種類のイベントによってどのメソッドおよびデータ構造が呼び出されるのかを判定する。その後、チャネルマネージャ562は、コンポーネントアセンブリ690を形成するのに必要なメソッドおよびデータ構造を取得させるコールを（例えば、安全なデータベースマネージャ566に）発行する。これらのコールされたメソッドおよびデータ構造（例えば、ロードモジュール1100、UDE 1200および／またはMDE 1202）は、（必要であれば）暗号化／復号化マネージャ556を用いてそれぞれ復号化され、その後、鍵およびタグマネージャ558を用いてそれぞれ有効性が検査される。チャネルマネージャ562は、あらゆる必要な「ジャンプテーブル」を構築してエレメントを実効的に単一の凝集性（cohesive）実行可能物に「リンク」あるいは「結合」し、これにより、ロードモジュールはコンポーネントアセンブリにおいてデータ構造および他のあらゆるロードモジュールを参照できる。その後、チャネルマネージャ562は、LMEM 568に実行可能物をアクティブタスクとしてロードさせるコールを発行し得る。

図15は、チャネル594が別のチャネルを参照し得ることを示している。チャネルマネージャ594によって任意の数のチャネル594を形成して、互いにインタラクトさせることが可能である。

好適な実施形態における「チャネルヘッダ」596は、チャネルイベント資源か

らイベントをキューイングし、これらのイベントを処理し、そして「チャネル詳細レコード」において指定された適切なタスクを、処理のために開放するデータ構造および関連制御プログラム（あるいはそれを参照するもの）である。好適な実

施形態における「チャネル詳細レコード」は、あるイベントを、そのイベントに関連付けられた「スワップブロック」（即ち、タスク）にリンクする。「スワップブロック」は、そのイベントを正しく処理するのに必要とされる１つ以上のロードモジュール1100、UDE 1200および秘密データ領域を参照し得る。チャネルが応答できる異なるイベントのそれぞれについて、１つのスワップブロックおよびこれに対応するチャネル詳細項目が作成される。

好適な実施形態において、チャネルサービスマネージャ562は、以下の（内部）コールをサポートすることにより、チャネル562の作成および維持をサポートし得る。

コール名	ソース	説明
「書込みイベント」	Write	チャネルによるレスポンスのためにチャネルにイベントを書き込む。このようにして書込みイベントコールは、発信者があるイベントをそのチャネルに関連付けられたイベントキューに挿入することを可能にする。次に、そのイベントはチャネル594によって処理される。
「結合項目」	Ioctl	適切な処理アルゴリズムを用いて項目をチャネルに結合させる。結合項目コールは、（例えば、あるチャネルに関連付けられた１つ以上のスワップブロックを作成するために）発信者がVDE項目IDをチャネルに結合させることを可能にする。このコールは、個々のスワップブロックのコンテンツを操作(manipulate)し得る。
「開放項目」	Ioctl	適切な処理アルゴリズムを用いて項目をチャネルから開放する。開放項目コールは、項目のスワップブロックへの結合を発信者が解くことを可能にする。このコールは、個々のスワップブロックのコンテンツを操作(manipulate)し得る。

SPE RPCマネージャ550

図12を参照しながら説明したように、好適な実施形態においては、ROS 602のアーキテクチャは遠隔プロシージャコールに基づいている。ROS 602は、それぞれRPCサービスインターフェース（「RSI」）をRPCマネージャに提示する（present）サービス間においてRPCコールの引渡しを行うRPCマネージャ732を有する。好適な実施形態においては、SPE 503（HPE 655）もまた、同じRPCコンセプトに基づいて形成される。SPE 503（HPE 655）は、それぞれがRSIをSPE（HPE）の内部にあるRPCマネージャ550に提示する複数の内部モジュール式サービスプロバイダを有し得る。これらの内部サービスプロバイダは、RPCサービス要求を用いて、互いと、および／またはROS RPCマネージャ732と（よって、ROS 602によって提供される他のあらゆるサービスおよび外部のサービスと）通信し得る。

SPE 503（HPE 655）内のRPCマネージャ550は、図12に示されるRPCマネージャ732と同じではないが、SPE（HPE）内で同様の機能を行う。即ち、RPCマネージャ550は、RPC要求を受信し、それらを、その要求を実行するサービスによって提示されるRSIに引き渡す。好適な実施形態においては、ROSRPCマネージャ732と外界（即ち、SPEデバイスドライバ736）との間で、SPE（HPE）カーネル／ディスパッチャ552を介した要求の引渡しが行われる。カーネル／ディスパッチャ552は特定のRPC要求をそれ自身でサービスすることができるが、一般には、受信した要求をRPCマネージャ550に引き渡して、SPE（HPE）の内部の適切なサービスにルーティングする。代替的な実施形態においては、要求は、ROS RPCマネージャ732を介してルーティングするのではなく、HPE、SPE、API、通知書インターフェースおよび他の外部サービスの間で直接引き渡される。どの実施形態を用いるかの決定は、システムの尺度可能性（scalability）の一部である。即ち、多様なトラフィック負荷（traffic load）およびシステムコンフィギュレーションの下では、ある実施形態が別の実施形態よりも効率的になる。サービスによる応答（およびサービス自身が生成し得る付加的なサービス要求）は、RPCマネージャ550に提供されて、SPE 503（HPE 655）の内部あるいは外部にある他のサービスにルーティングされる。

SPE RPCマネージャ550およびその一体化されたサービスマネージャは、RPCサー

ビステーブルおよび任意に省略可能なRPCディスパッチテーブルの２つのテーブルを使用して遠隔プロシージャコールをディスパッチする。RPCサービステーブルは、特定のサービスへの要求がどこにルーティングされて処理されるのかを示す。好適な実施形態において、SPU RAM 534aあるいはNVRAM 534b内で構築されるこのテーブルは、SPU 500内に「登録された」各RPCサービスを列記したものである。RPCサービステーブルの各行は、サービスIDと、その場所およびアドレスと、制御バイトとを有する。単純なインプリメンテーションの場合、制御バイトは、サービスが内部で提供されるのか外部で提供されるのかを表すのみである。より複雑なインプリメンテーションの場合、制御バイトはサービスのインスタンス

を表し得る（例えば、多重タスク処理環境において各サービスは複数の「インスタンス」を有し得る）。好適な実施形態において、ROS RPCマネージャ732およびSPE 503はRPCサービステーブルの対称的なコピーを有し得る。RPCサービスがRPCサービステーブル内で見つからない場合、SPE 503は、それを拒否(reject)するか、あるいは、それをサービスのためにROS RPCマネージャ732に引き渡す。

SPE RPCマネージャ550はRPCサービステーブルからの要求を受け入れて、特定のサービスに関連する内部優先順位に従ってその要求を処理する。SPE 503においては、RPCサービステーブルはRPCディスパッチテーブルによって拡張される。好適な実施形態のRPCディスパッチテーブルは、SPE 503によって内部でサポートされる各RPCサービスについてのロードモジュールリファレンスのリストとしてまとめられる(organized)。テーブルの各行は、コールをサービスするロードモジュールIDと、外部の発信者がそのコールを発することが可能かどうかおよびそのコールをサービスするのに必要なロードモジュールがSPU 500内に恒久的に常駐しているかどうかを表す制御バイトとを有している。SPUファームウェア508がSPU 500内にロードされている場合、RPCディスパッチテーブルはSPU ROM 532（あるいはEEPROM）内に構築され得る。RPCディスパッチテーブルがEEPROM内にある場合、RPCディスパッチテーブルは、ロードモジュール位置およびバージョン制御問題無しでサービスに対する更新を柔軟に許可する。

好適な実施形態においては、SPE RPCマネージャ550は先ず、RPCサービステーブルに対する(against)サービス要求を参照することにより、その要求をサービスし

得るサービスマネージャの位置を決定する。その後、RPCマネージャ550は、サービス要求を、適切なサービスマネージャにルーティングして実行(action)する。サービス要求は、SPE 503内のサービスマネージャによって、RPCディスパッチテーブルを用いて処理され、これにより、要求がディスパッチされる。RPCマネージャ550によってRPCディスパッチテーブル内のサービスリファレンスの位置が決定されると、その要求をサービスするロードモジュールがコールされ、ロードモジュール実行マネージャ568を用いてロードされる。ロードモジュール実行マネ

ージャ568は、要求される全てのコンテキストコンフィギュレーションを行った後、要求されるロードモジュールに制御を引き渡すか、あるいは、そうする必要がある場合、制御を外部管理ファイル610からロードする要求を初めに発行してもよい。

SPU時間ベースマネージャ554

時間ベースマネージャ554は、リアルタイムクロック（「RTC」）528に関するコールをサポートする。好適な実施形態において、時間ベースマネージャ554は常に、ロードされており、時間ベースの要求に応答する準備ができている。

以下の表は、時間ベースマネージャ554によってサポートされ得る基本コールの例をリストにしたものである。

コール名	説明
独立要求	
時間獲得	時間を返す（ローカル、GMT、あるいはチック）
時間設定	RTC 528に時間を設定する。このコマンドへのアクセスはVDE管理者に対しては制限され得る。
時間調節	RTC 528内の時間を変更する。このコマンドへのアクセスはVDE管理者に対しては制限され得る。
時間パラメータ設定	GMT／ローカル時間変換と、現在許可されているユーザによるRTC 528時間の調節量を設定する。
チャネルサービスマネージャ要求	
時間結合	タイマサービスをイベント資源としてのチャネルに結合させる。
時間開放	イベント資源としてのチャネルからタイマサービスを開放する。
アラーム設定	アラーム通知を特定の時間に設定する。アラームの時間になると、ユーザはアラームイベントによって通知を受ける。この要求のパラメータは、イベント、頻度、およびアラームに対して要求される処理を決定する。
アラーム解除	要求されているアラーム通知を取り消す。

SPU暗号化／復号化マネージャ556

暗号化／復号化マネージャ556は、SPE 503／HPE 655によってサポートされる

様々な暗号化／復号化技術に対するコールをサポートする。暗号化／復号化マネージャ556は、SPU 500内のハードウェアベース暗号化／復号化エンジン522によってサポートされ得る。SPU暗号化／復号化エンジン522によってサポートされていない暗号化／復号化技術は、暗号化／復号化マネージャ556によってソフトウェアとして提供される。一次バルク暗号化／復号化ロードモジュールは、好ましくは常にロードされており、他のアルゴリズムのために必要なロードモジュールは好ましくは必要に応じてページインされる。従って、一次バルク暗号化／復号化アルゴリズムがDESである場合、SPE 503／HPE 655のRAM 534a内に恒久的に常駐している必要があるのはDESロードモジュールのみである。

以下に示すのは、好適な実施形態において、暗号化／復号化マネージャ556によってサポートされるRPCコールの例である。

コール名	説明
PK暗号化	PK（公開鍵）アルゴリズムを用いてブロックを暗号化する。
PK復号化	PKアルゴリズムを用いてブロックを復号化する。
DES暗号化	DESを用いてブロックを暗号化する。
DES復号化	DESを用いてブロックを復号化する。
RC-4暗号化	RC-4（あるいは他のバルク暗号化）アルゴリズムを用いてブロックを暗号化する。
RC-4復号化	RC-4（あるいは他のバルク暗号化）アルゴリズムを用いてブロックを復号化する。
DESインスタンス初期化	DESインスタンスを初期化する。
RC-4インスタンス初期化	RC-4インスタンスを初期化する。
MD5インスタンス初期化	MD5インスタンスを初期化する。
MD5ブロック処理	MD5ブロックを処理する。

引き渡されるコールパラメータには、使用する鍵、モード（暗号化あるいは復号化）、必要とされるあらゆる初期化ベクトル、所望の暗号的処理（例えば、フィードバックの種類）、使用する暗号的インスタンスの識別子（identification）、ならびに、暗号化あるいは復号化するブロックの開始アドレス、デスティネーションアドレスおよび長さが含まれ得る。

SPE鍵およびタグマネージャ558

SPE鍵およびタグマネージャ558は、鍵保管（key storage）、鍵および管理ファイルタグルックアップ、鍵旋回、ならびに、ランダム鍵、タグおよび取引番号の生成のコールをサポートする。

以下の表は、SPE／HPE鍵およびタグマネージャサービス558コールのリストの一例を示す。

コール名	説明
鍵要求	
鍵獲得	要求されている鍵を検索する。
鍵設定	特定の鍵を設定（格納）する。

鍵生成	特定のアルゴリズムについての鍵（対）を生成する。
旋回鍵生成	特定の旋回アルゴリズムおよびアルゴリズムパラメータブロックを用いて鍵を生成する。
旋回アルゴリズム獲得	特定の旋回アルゴリズムについての現在設定されている（デフォールト）旋回パラメータを返す。
旋回アルゴリズム設定	特定の旋回アルゴリズムについての旋回パラメータを設定する（返されたコンテンツを読むために、コールしているルーチンはタグを提供しなければならない。）。
タグ要求	
タグ獲得	特定のVDE項目IDについての有効性（あるいは他の）タグの有効性を獲得する。
タグ設定	特定のVDE項目IDについての有効性（あるいは他の）タグの有効性を既知の値に設定する。
ハッシュブロック数算出	特定のVDE項目IDについての「ハッシュブロック数」を算出する。
ハッシュパラメータ設定	ハッシュパラメータおよびハッシュアルゴリズムを設定する。ハッシュテーブルの再同期化を強制する。
ハッシュパラメータ獲得	現在のハッシュパラメータ／アルゴリズムを検索する。
管理ファイルの同期化	管理ファイルを同期化し、VDE管理者用にリザーブされたテーブルで見つかった情報に基づいてハッシュブロックテーブルを再形成する。

好適な実施形態において、鍵およびタグはSPE 503（HPE 655）内で安全に生成され得る。典型的に、鍵生成アルゴリズムは、サポートされている暗号化の各種類について特異的である。生成された鍵は、使用前に、暗号的弱点についてチェックされる。好ましくは、鍵およびタグマネージャ558に鍵、タグおよび／または取引番号を生成させる要求は、その入力パラメータとしてある長さをとる。その要求は、出力として、要求された長さの乱数（あるいは他の適切な鍵値）を生成

する。

鍵およびタグマネージャ558は、SPU 500内の鍵保存領域の特定の鍵およびSPUの外部に格納されているあらゆる鍵を検索するコールをサポートし得る。これらのコールの基本フォーマットは、鍵の種類および鍵番号によって鍵を要求するというものである。鍵の多くは、VDE管理者との接触によって定期的に更新され、NVRAM 534bあるいはEEPROMにおいてSPU 500内に保持される。なぜなら、これらのメモリは安全、更新可能、且つ不揮発性だからである。

SPE 503／HPE 655は、公開鍵タイプの鍵およびバルク暗号化タイプの鍵の両方をサポートし得る。SPU 500によって格納され、鍵およびタグマネージャ558によって管理される公開鍵（PK）暗号化タイプの鍵には、例えば、デバイス公開鍵、デバイス秘密鍵、PK証明書、および証明書の公開鍵が含まれ得る。一般に、公開鍵および証明書は、そうすることが望まれる場合、外部の非保証（non-secured）メモリに格納され得るが、デバイス秘密鍵および証明書の公開鍵は、内部のSPU 500EEPROMあるいはNVRAM 534b内にのみ格納されるべきである。SPU 500によって使用されるバルク暗号化鍵の種類には、例えば、汎用バルク暗号化鍵、管理的オブジェクト秘密ヘッダ鍵、静止オブジェクト秘密ヘッダ鍵、移動オブジェクト秘密ヘッダ鍵、ダウンロード／初期化鍵、バックアップ鍵、追跡鍵（trail keys）、および管理ファイル鍵が含まれ得る。

上記のように、好適な実施形態の鍵およびタグマネージャ558は、鍵を調節あるいは旋回して新たな鍵を作る要求をサポートする。この新たな鍵は、例えばサイトおよび／または時間に依存する確定的な方法で作成される。鍵の旋回は、鍵と何らかの入力パラメータセットに作用して新たな鍵を生み出すアルゴリズム的プロセスである。鍵の旋回を利用すれば、例えば、付加的な鍵保存スペースを生じることなく使用できる鍵の数を増やすことができる。また、鍵の旋回は、例えば、リアルタイムRTC 528の値をパラメータとして組み込んで鍵を「経時変化させる」プロセスとしても利用できる。鍵の旋回を利用して、サイトIDの局面をパラメータとして組み込んで鍵をサイト特異的にすることが可能である。

鍵およびタグマネージャ558は、タグの生成および管理に関するサービスをも提供し得る。好適な実施形態において、取引およびアクセスタグは、好ましくは

（例えば、SPU 500のNVRAM 534b内の）プロテクトされたメモリ内にSPE 503（HPE 655）によって格納される。これらのタグは、鍵およびタグマネージャ558によって生成され得る。これらのタグは、例えば、データエレメントへのアクセス権のチェック、データエレメントの有効性検査および相互関連付けを行うために使用され得る。例えば、これらのタグを用いて、安全なデータ構造のコンポーネントがSPU 500の外部によって不正改変されていないことを確実にすることができる。鍵およびタグマネージャ558は、追跡取引タグおよび通信取引タグをもサポートし得る。

SPU要約サービスマネージャ560

SPE 503は、SPU 500内の再プログラム可能不揮発性メモリおよび／または安全なデータベース610内に監査追跡を維持する。この監査追跡は、金融目的の予算活動の監査要約と、SPUが使用するセキュリティ要約で構成され得る。SPUに対して要求がなされると、その要求が生じたことが記録（logs）され、そして、その要求が成功したか失敗したかが付記される。成功した要求は全て合計されて、種類毎にSPU 500内に格納される。以下に挙げるするエレメントを含む失敗情報は、その失敗の詳細とともにセーブされ得る。

アクセス失敗に関するSPE内に保持される制御情報
オブジェクトID
ユーザID
失敗の種類
失敗の時刻

この情報を分析して、クラッキングの試み（cracking attempt）の検出、あるいは、予期される（および予算編成された）基準（norm）から外れた使用パターンの決定を行うことができる。SPU 500内の監査追跡歴（audit trail histories）は、監査が適切なパーティに報告されるまで維持される。これにより、正当な失敗分析（legitimate failure analysis）およびSPUを暗号解析する試みを付記することが

可

能になる。

要約サービスマネージャ560は、この内部要約監査情報の格納および維持を行い得る。この監査情報を用いて、セキュリティ突破口(security breaches)あるいはSPE 503の動作の他の局面のチェックを行うことができる。イベント要約は、電子機器600の不正使用を特定し、可能であればこれを制限するために、SPE 503（HPE 655）あるいはVDE管理者によって維持、分析および使用される。好適な実施形態においては、このようなパラメータは安全なメモリ内（例えば、SPU 500のNVRAM 534b内）に格納され得る。

好適な実施形態において、要約サービスが使用される基本構造は2つある。その内の1つ（「イベント要約データ構造」）は、VDE管理者特異的であり、イベントを追跡する。イベント要約構造は、VDE管理者との定期的な接触の間、維持および監査され得る。もう1つは、VDE管理者および／または配布者によって、全体予算のために使用される。VDE管理者は、電子機器600が初期化される時点で、イベント要約および全体予算要約の登録を行い得る。全体予算要約は、VDE管理者に報告され、VDE管理者によって、（例えば）安全な管理ファイル610の不正行為(corruption)があった場合に、消費された予算の配布を決定するために使用される。適切なパーミッションを受け取る参加者は、そのプロセス（例えば、特定の予算）を、要約サービスマネージャ560を用いて登録し得る。その後、要約サービスマネージャ560は、（例えば、NVRAM 534b内の）プロテクトされたメモリスペースをリザーブするとともに、所望の使用および／またはアクセスパラメータを維持し得る。各要約へのアクセスおよびその改変は、それ自身のアクセスタグによって制御できる。

以下の表は、PPE要約サービスマネージャ560サービスコールのリストの一例を示す。

コール名	説明
要約情報の作成	ユーザが、このサービスをユーザが要求することを許可する「チケット」を有する場合に、要約サービスを生成する。
値獲得	要約サービスの現在の値を返す。この要求を使用するために

	は、発信者は適切なタグ（および／または「チケット」）を提示しなければならない。
値設定	要約サービスの値を設定する。
インクリメント	特定の要約サービス（例えば、スカラー計量要約データ領域(scalar meter summary data area)）をインクリメントする。この要求を使用するためには、発信者は適切なタグ（および／または「チケット」）を提示しなければならない。
破棄	ユーザが、このサービスをユーザが要求することを許可する「チケット」を有する場合に、特定の要約サービスを破棄する。

好適な実施形態においては、イベント要約データ構造は固定イベント番号を使用して、ルックアップテーブル内への索引付けを行う。ルックアップテーブルは、カウンタあるいはカウンタ＋リミットとして構成され得る値を有する。カウンタモードは、VDE管理者によって、デバイスの使用法を決定するために用いられ得る。リミットモードを利用して、電子機器600の不正改変および不正使用の試みを制限することができる。リミットを越えると、SPE 503（HPE 655）は、それがVDE管理者によってリセットされるまでの間、ユーザ要求のサービスを拒否することになる。システム規模のイベント要約プロセスに対するコールは、好ましくは、関係するイベントを処理する全てのロードモジュール内にビルトインされる。

以下の表は、好適な実施形態のイベント要約データ構造によって別々に計量され得るイベントの例を示す。

イベントの種類	
成功イベント	初期化首尾良く完了。
	ユーザ認証受諾(accepted)。
	通信確立。
	チャネルロードを特定の値に設定。
	復号化完了。

	鍵情報更新。
	新規予算作成または既存予算更新。
	新課金情報生成あるいは既存課金更新。
	新計量セットアップあるいは既存計量更新。
	新PERC作成あるいは既存PERC更新。
	新オブジェクト登録。
	管理的オブジェクト首尾良く処理完了。
	監査処理首尾良く完了。
	他の全てのイベント。
失敗イベント	初期化失敗。
	認証失敗。
	通信試行失敗。
	チャネルロード要求失敗
	有効性検査試行不成功。
	付属項目へのリンク、相関タグマッチ失敗。
	承認試行失敗。
	復号化試行失敗。
	利用可能な予算が、要求されたプロシージャの完了に不十分。
	監査行われず。
	管理的オブジェクトの処理、正しく行われず。
	他の失敗イベント

好適な実施形態の要約サービスマネージャ560によって維持されるもう１つの

「全体通貨予算」要約データ構造は、VDE電子機器600の登録を可能にする。初めのエントリは、全体通貨予算消費値(overall currency budget consumed value)のために用いられ、VDE管理者によって登録される。VDE管理者は、先ずSPE 503（HPE 655）を初期化する。特定の通貨消費ロードモジュールと、消費通貨予算の監査プロセスを完了する監査ロードモジュールとは、通貨消費値を更新するよう

に要約サービスマネージャ560をコールし得る。特別承認ロードモジュールは全体通貨要約へのアクセスを有し得、付加的要約は個々のプロバイダによって登録され得る。

SPE認証マネージャ／サービス通信マネージャ564

認証マネージャ／サービス通信マネージャ564は、ユーザパスワードの有効性検査ならびに「チケット」の生成および有効性検査のコールをサポートする。認証マネージャ／サービス通信マネージャ564はまた、SPE 503と外部ノードあるいはデバイス（例えば、VDE管理者あるいは配布者）との間の安全な通信をサポートする。認証マネージャ／サービス通信マネージャ564は、好適な実施形態における認証関連サービス要求の以下の例をサポートし得る。

コール名	説明
ユーザサービス	
ユーザ作成	新たなユーザを作成し、ネームサービスマネージャ752が使用するネームサービスレコード（NSR）を格納する。
ユーザ認証	システムの使用についてのユーザ認証を行う。この要求は、発信者を特定のユーザIDとして認証する。グループメンバーシップも、この要求によって認証される。認証は、ユーザ用の「チケット」を返す。
ユーザ削除	ユーザのNSRおよび関連レコードを削除する。
チケットサービス	
チケット生成	１つ以上のサービスを使用するための「チケット」を生成する。
チケット認証	「チケット」の認証を行う。

上記の表に含まれていないのは、安全な通信サービスに対するコールである。マネージャ564によって提供される安全な通信サービスは、（例えば、それが望まれる場合、ローレベルサービスマネージャ582と関連して）公開鍵（あるいは他の）

チャレンジーレスポンスプロトコルに基づく安全な通信を提供し得る。このプロトコルについては、本明細書の他の箇所により詳細に説明されている。機器が複数のユーザによって使用され得る場合、チケットは、電子機器600に関してユーザを識別する。チケットは、チケット交付プロトコル（例えば、Kerberos）を用いて、VDEソフトウェアアプリケーションによって要求され、VDEソフトウェアアプリケーションに返される。VDEコンポーネントは、特定のサービスが許可されるようにチケットが提示されることを要求し得る。

SPE安全データベースマネージャ566

安全なデータベースマネージャ566は、SPE 503の外部にあるメモリの安全なデータベース610内の安全なデータベースレコードを検索、維持、および格納する。安全なデータベースファイル610の多くは、暗号形式である。従って、安全なデータベースマネージャ566によって検索された全ての安全な情報は、使用前に

、暗号化／復号化マネージャ556によって復号化されなければならない。安全な実行環境の外部に格納されなければならない、SPE 503（HPE 655）が生成する安全な情報（例えば、使用のレコード）もまた、安全なデータベースマネージャ566によってそれらが安全なデータベースファイル610内に格納される前に、暗号化／復号化マネージャ556によって暗号化される。

SPE 503内にロードされるVDE項目のそれぞれについて、好適な実施形態の安全なデータベースマネージャ566は、提供された項目が現在の項目であることを確実にするために、VDE項目IDのマスタリストをサーチし、その後、その項目内の取引タグに対して対応取引タグをチェックし得る。安全なデータベースマネージャ566は、VDE項目IDおよび取引タグのリストを「ハッシュ構造」で保持することができ、これらを、SPE 503にページインして適切なVDE項目IDの位置を迅速に決定することができる。比較的小規模のシステムにおいては、ルックアップテーブルアプローチが用いられ得る。いずれの場合も、リストは、VDE項目IDの位置が迅速に決定できるページング可能な構造として構成されるべきである。

「ハッシュベース」アプローチを用いて、リストを「ハッシュバケツ」にソートし得る。その後「ハッシュバケツ」にアクセスして、より高速且つ効率的なリスト内の項目の位置決定を行うことができる。「ハッシュベース」アプローチにおいては、VDE項目IDは、完全な項目IDの部分集合で「ハッシュされ」、そして、「ハッシュされた」テーブルのページとしてまとめられる。「ハッシュされた」ページのそれぞれは、VDE項目IDの残りと、そのページに関連する各項目の現在の取引タグとを含み得る。「ハッシュ」テーブルページ番号は、配布ID、項目ID、サイトID、ユーザID、取引タグ、クリエータID、種類および／またはバージョン等のVDE項目IDのコンポーネントから求められ得る。ハッシュ処理アルゴリズム（アルゴリズム自身およびハッシュされるパラメータの両方）は、最適なハッシュページの使用を提供するように、VDE配布者によってサイト毎に構成可能であり得る。ハッシュページ構造の例を以下に示す。

フィールド
ハッシュページヘッダ
配布者ID
項目ID
サイトID
ユーザID
取引タグ
ハッシュページエントリ
クリエータID
項目ID
種類
バージョン
取引タグ

この例において、各ハッシュページは、同一の配布者ID、項目ID、およびユーザIDフィールド（サイトIDは所与の電子機器600について固定される）を有するVDE項目IDおよび取引タグの全てを含み得る。従って、これらの４つの情報はハッシュアルゴリズムパラメータとして使用され得る。

「ハッシュ」ページは、それら自身が頻繁に更新される可能性があり、「ハッシュ」ページがロードされる度にチェックされる取引タグを有するべきである。また、取引タグは「ハッシュ」ページが書き出される度に更新され得る。

ハッシュベースアプローチの代替物として、更新可能項目の数を小さく抑えることが可能な場合（専用消費者電子機器600の場合のように）、更新可能項目のそれぞれにVDE項目IDの一部として固有のシーケンシャルサイトレコード番号を割り当てることによって、ルックアップテーブルアプローチの使用が可能になり得る。項目毎に必要なのは少数の取引タグのバイトのみであり、頻繁に更新可能な全ての項目のテーブル取引タグがSPU NVRAM 534b等のプロテクトされたメモリ内に保持され得る。

乱数値発生器565

乱数値発生器マネージャ565は、乱数値を発生し得る。ハードウェアベースSPU乱数値発生器542が存在する場合、乱数値発生器マネージャ565はハードウェアベースSPU乱数値発生器542を用いて乱数値の発生を助長することができる。

他のSPE RPCサービス592

他の承認されたRPCサービスは、それらにそれら自身をRPCサービステーブル内に「登録」させて、それらのエントリをRPCディスパッチテーブルに追加することによって、SPU 500内に含めることができる。例えば、１つ以上のコンポーネントアセンブリ690を用いて、付加的なサービスを、SPE 503の一部分およびそれに関連するオペレーティングシステムとして提供することができる。これらのテーブルに登録されていない要求は、外部サービスのために、SPE 503（HPE 655）の外部に引き渡される。

SPE 503の性能の考察

SPE 503（HPE 655）の性能は、

C　使用するコンポーネントアセンブリの複雑さ

C　同時コンポーネントアセンブリ処理の数

C　利用可能な内部SPUメモリの容量

C　ブロック暗号化／復号化のアルゴリズムのスピード

の関数である。

同時コンポーネントアセンブリ処理の数とともに、コンポーネントアセンブリの複雑さは、おそらく性能を決定する主要な要因である。これらの要因の組合わせによって、どの時点においてもSPU 500内に常駐していなければならないコードおよびデータの量（最小デバイスサイズ）が決定され、これにより、プロセスを何個のデバイスサイズ「チャンク」に分割しなければならないのかについても決定される。セグメント化は、本質的に、より単純なモデルよりもランタイムサイズを増大させる。無論、ずっと少ない容量のRAM 534を用いて、機能限定バージョンのSPU 500を実現することが可能である。上記のような「合計（aggregate）」ロードモジュールは、VDE構造を構成する際の柔軟性を排除するとともに、参加者が個々に、更新しなければ分離するエレメントを更新する能力をも制限する

が、より小さな最小デバイスサイズをもたらし得る。非常に単純な計量バージョンのSPU 500を、最小デバイス資源で動作するように構築することができる。

SPU 500の内部にあるRAM 534の容量がSPE 503の性能に与える影響は、おそらくSPUの他のあらゆる局面よりも大きい。VDEプロセスの柔軟な性質は、多数のロードモジュール、メソッド、およびユーザデータエレメントの使用を可能にする。SPU 500内のROM 532内にこれらの項目を多数保存するのは非実用的である。特定のVDEプロセスをサポートするのに必要なコードおよびデータ構造のほとんどは、そのプロセスが呼び出された時に、その特定のVDEプロセスのためにSPU 500内にダイナミックにロードされる必要がある。その後、SPU 500内のオペレーティングシステムは、そのプロセスを行うために必要なVDE項目をページインし得る。SPU 500内のRAM 534の容量は、あるVDEプロセスを実行するために必要なページスワップの数と、任意の単一VDEロードモジュール＋要求されるデータがどれ位大きくなり得るかとを直接的に決定する。SPU I/Oスピード、暗号化／復号化スピード、および内部メモリ532および534の容量は、そのデバイスにおいて要求されるページスワップの数に直接的に影響する。安全でない外部メモリは、スワップされたページがSPU 500内にロードされる際の待ち時間を低減し得るが、それでも、暗号化

／復号化に関する重大な不都合を各ページについて生じるであろう。

セキュリティを維持するために、SPE 503は、サポートしているSPU 500の外部にある記憶装置にスワップアウトされる各ブロックを暗号化し且つ暗号学的に封印しなければならなず、また同様に、SPU 500にブロックがスワップインされる際には、各ブロックを復号化し、その暗号学的封印を検証し、そして、有効性検査を行わなければならない。各スワップブロックについてのデータ移動および暗号化／復号化オーバーヘッドは、SPE性能に非常に大きな影響を与える。

そのプロセッサが暗号化／復号化エンジン522を介したデータの移動を行うものでない場合、そのプロセッサによってサポートされるSPE 503の性能にSPUマイクロプロセッサ520の性能が与える影響は重大ではないかもしれない。

VDE安全データベース610

ＶＤＥ １００は、別々に配送可能なＶＤＥエレメントを、各ＶＤＥ電子機器６１０に交付される安全な（例えば、暗号化された）データベース６１０内に格納する。好適な実施形態において、データベース６１０は、３つの基本的なクラスのＶＤＥ項目を格納および／または管理し得る。

ＶＤＥオブジェクト

ＶＤＥプロセスエレメント、および

ＶＤＥデータ構造

以下の表は、安全なデータベース６１０内に格納される、あるいは安全なデータベース６１０内に格納された情報によって管理されるＶＤＥ項目の一部の例をリストにしたものである。

クラス		簡単な説明
オブジェクト	コンテンツオブジェクト	コンテンツのコンテナを提供する。
	管理的オブジェクト	VDE 100の処理を維持するために使用する情報のコンテナを提供する。

	移動オブジェクト	コンテンツおよび制御情報のコンテナを提供する。
	スマートオブジェクト	（ユーザが特定した）プロセスおよびデータのコンテナを提供する。
プロセスエレメント	メソッドコア	イベントを制御メカニズムおよびパーミッションに関連させる(relate)メカニズムを提供する。
	ロードモジュール（「LM」）	（不正改変不可能な）実行可能物コードを秘密保護する(secure)。
	メソッドデータエレメント(「MDE」	メソッドを制御／カスタマイズするために使用される独立配送可能なデータ構造。
データ構造	パーミッションレコード（「PERC」	オブジェクトを使用するパーミッション。即ち、コンポーネントアセンブリを形成する「ブループリント」。
	ユーザデータエレメント（「UDE」	ロードモジュールに関連して使用される情報を格納するための基本データ構造。
	管理的データ構造	管理的な情報を維持するためにVDEノードによって使用される。

各電子機器600は、VDE項目を安全に維持する安全なデータベース610のインスタンスを有し得る。図16は、安全なデータベース610の一例を示す。この例において示される安全なデータベース610は、以下のVDEプロテクトされた項目を含む。

C　　１つ以上のPERC 808、

C　　メソッド1000（静的および動的なメソッド「コア」1000およびMDE 1202を含む）、

C　　静的UDE 1200aおよび動的UDE 1200b、ならびに

C　　ロードモジュール1100

安全なデータベース610は、管理上の目的で使用および維持される以下の付加的なデータ構造をも含み得る。

Ｃ　　１つ以上のVDEオブジェクトを有するオブジェクト記憶装置728を参照する「オブジェクトレジストリ」450

Ｃ　　ネームサービスレコード452、および

Ｃ　　コンフィギュレーションレコード454（サイトコンフィギュレーションレコード456およびユーザコンフィギュレーションレコード458を含む）

好適な実施形態において、安全なデータベース610は、VDEオブジェクト300を含んでおらず、例えば、ファイルシステム687上および／または別個のオブジェクト容器728内に格納されたVDEオブジェクトを参照する。しかし、VDEプロテクトされた情報を理解する適切な「第一歩」は、VDEオブジェクト300の説明であろう。

VDEオブジェクト300

VDE 100は、コンテンツをカプセル化するメディア独立型コンテナモデルを提供する。図17は、好適な実施形態によって提供されるオブジェクト300の「論理」構造あるいはフォーマット800の一例を示す。

好適な実施形態において用いられる図17に示す一般化された「論理オブジェクト」構造800は、現在使用されているあらゆるメディアよるデジタルコンテンツの配送をサポートする。好適な実施形態において、「論理オブジェクト」は、コンテンツと、上記コンテンツの使用を操作（manipulate）、記録、および／または制御するために用いられるコンピュータソフトウェアおよび／またはメソッドと、上記コンテンツおよび／または上記コンピュータソフトウェアおよび／またはメソッドに適用可能なパーミッション、制限、管理的制御情報および／または要件とのことを集合的に指し得る。論理オブジェクトは、格納される場合もされない場合もあり、また、あらゆる所与の電子機器600に存在するあるいはアクセス可能である場合もそうでない場合もある。論理オブジェクトのコンテンツ部分は、１つ以上のオブジェクト内に含まれる、含まれない、あるいは部分的に含まれる情報として組織化され得る。

簡潔に述べれば、好適な実施形態において、図17の「論理オブジェクト」構造800は、公開ヘッダ802と、秘密ヘッダ804と、１つ以上のメソッド1000を有する「秘密ボディ（private body）」806と、（１つ以上の鍵ブロック810を含み得る）

バー

ミッションレコード（PERC）808と、１つ以上のデータブロックあるいは領域812とを含む。これらのエレメントは、「コンテナ」302内に「梱包(packaged)」され得る。好適な実施形態において、この一般化された論理オブジェクト構造800は、そのコンテンツの種類および位置によって分類される異なる種類のVDEオブジェクト300に用いられる。

「コンテナ」の概念は、コンテンツの利用あるいは管理的な種類のアクティビティの実行に要求されるエレメントの収集物(collection)を名付けるのに好都合なメタファーである。コンテナ302は、典型的に、識別情報(identifying information)、制御構造およびコンテンツ（例えば、プロパティあるいは管理的データ）を含む。「コンテナ」という用語はしばしば(例えば、Bento/OpenDocおよびOLE)用いられ、コンピュータシステムの２次記憶装置システムに格納された情報、あるいは、「サーバの」２次記憶装置システム上の通信ネットワークを介してコンピュータシステムにアクセス可能な情報の収集物を表す。好適な実施形態によって提供される「コンテナ」320は、このように限定あるいは制限されるものではない。VDE 100の場合、この情報は、一緒に格納されている必要はなく、同時に受信される必要はなく、同時に更新される必要はなく、単一のオブジェクトに対してのみ使用される必要はなく、あるいは同一のエンティティによって所有されている必要はない。むしろ、VDE 100においては、コンテナ概念が広げられ、一般化されて、ケーブルを介して一斉通信によって(by broadcast)電子機器に引き渡された、あるいは他の電子通信手段によって通信されたリアルタイムコンテンツおよび／またはオンラインインタラクティブコンテンツもが含まれる。

従って、「完全な」VDEコンテナ302あるいは論理オブジェクト構造800が、任意の時点で、ユーザの位置（あるいはそのことに関する他のあらゆる位置）に存在しないかもしれない。「論理オブジェクト」は、一度に全て存在するのではなくて、特定の期間（あるいは複数の期間）にわたって存在し得る。この概念は、重要なコンテナエレメントが、複数の位置としておよび／またはある順序だった(互いに重なっている、あるいは重なっていない)複数の期間にわたって存在し得

る「仮想コンテナ」の観念(notion)を含む。無論、VDE 100コンテナは、必要な制御構造およびコンテンツと一緒に格納されてもよい。これは、単一のコンテナ内に

存在する全てのコンテンツおよび制御構造から、ローカルにアクセス不可能なコンテンツあるいはコンテナ特異的制御構造に至る連続体を表す。

典型的に、オブジェクトを表すデータの少なくとも一部は暗号化されており、それゆえに、その構造は認知不可能であるが、PPE 650内では、論理的に、オブジェクトを「コンテナ」302として見ることができる。なぜなら、その構造およびコンポーネントが自動的に透明に復号化されるからである。

コンテナモデルはイベント駆動型プロセスおよび好適な実施形態によって提供されるROS 602と良好にマージする。このモデルにおいて、コンテンツは小さく管理し易いもの(piece)に容易に細分化(subdivided)されるが、暗号化されていないコンテンツに固有の構造的な濃厚さ(richness)を維持するように格納される。また、オブジェクト指向のコンテナモデル（Bento/OpenDocあるいはole等）は、必要なオペレーティングシステム一体コンポーネントを挿入するために、また、様々なコンテンツ特異的なメソッドを規定する(defining)ために必要な「フック」を多数提供する。

より詳細に述べると、好適な実施形態によって提供される論理オブジェクト構造800は、公開（あるいは暗号化されていない）ヘッダ802を含む。このヘッダ802は、オブジェクトを識別するとともに、オブジェクト内の権利の１人以上の所有者および／またはオブジェクトの１人以上の配布者をも識別する。秘密（あるいは暗号化された）ヘッダ804は、公開ヘッダ内の情報の一部あるいは全てを含み得、さらに、好適な実施形態においては、サービス情報交換所、VDE管理者、あるいはSPU 500によってユーザがオブジェクトのユーザとしての登録を行おうとする際にオブジェクト300の有効性を検査し、識別する付加的なデータを含む。あるいは、１人以上の権利所有者および／またはオブジェクトの配布者を識別する情報は、暗号化された形式で、暗号化されたヘッダ804内に、上記付加的な有効且つ識別的なデータとともに配置され得る。

論理オブジェクト構造800は、オブジェクト300の使用および配布を制御する１セットのメソッド1000（即ち、プログラムあるいはプロシージャ）を有するあるいは参照する「秘密ボディ」806をも含み得る。各オブジェクトに異なるメソッド1000を任意に組み込む能力は、VDE 100を高度に構成可能にするために重要である。

メソッド1000は、オブジェクト300に対してユーザ（それが適切な場合、配布者、クライアント管理者等を含む）が何ができて何ができないのかを規定する基本的な機能を行う。従って、他のオブジェクトがそれよりもずっと複雑な（例えば、課金および使用制限）メソッドによって制御され得る一方で、あるオブジェクト300には、（新聞発行から１週間の間その新聞を読むための新聞スタンド価格のように）固定期間の間、固定料金で無制限に見ることを許可する等の比較的簡単なメソッドが備わっている場合がある。

図17に示される論理オブジェクト構造800は、１つ以上のPERC 808をも含み得る。PERC 808は、オブジェクト300の使用を管理し(govern)、オブジェクトあるいはそのコンテンツにアクセスする、あるいはそれを使用するために用いられなければならないメソッドあるいはメソッドの組み合わせを特定する。あるオブジェクトについてのパーミッションレコード808は、オブジェクト300内に格納された暗号化コンテンツの内容にアクセスするための復号化鍵を格納することができる鍵ブロック810を含み得る。

オブジェクトのコンテンツ部分は、典型的には、データブロック812と呼ばれる部分に分割される。データブロック812は、コンピュータプログラム、画像、音声、VDE管理的情報等を含む「コンテンツ」等のあらゆる種類の電子情報を有し得る。データブロック812のサイズおよび数は、そのプロパティのクリエータによって選択され得る。データブロック812が全て同一のサイズである必要はない（サイズは、コンテンツの使用法、データベースフォーマット、オペレーティングシステム、セキュリティおよび／または他の要因(consideration)によって影響され得る）。オブジェクト内のデータブロック812のそれぞれについて少なくとも１つの鍵ブロック810を使用することによってセキュリティは高められるが

、そうすることは必須ではない。鍵ブロック810はまた、一貫してあるいは疑似ランダム式に、複数のデータブロック812の部分にまたがり得る(span)。このまたがり(spanning)は、オブジェクト300、データベース、あるいは他の情報エンティティ内に含まれる寸断されたあるいは見かけ上ランダムなコンテンツ片に対して１つ以上の鍵を適用することによって、さらなるセキュリティを提供し得る。

物理的メディアによっておよび／または「チャネル外」手段（例えば、受領後ある顧客から別の顧客に再配布される）によって配布されるオブジェクト300の多くは、鍵ブロック810を、その鍵ブロックによって保護されるコンテンツの転送に用いた同一のオブジェクト300内に含んでいない可能性がある。これは、VDEオブジェクトが、VDEノードの範囲(confines)の外から電子的にコピーできるデータを有し得るからである。コンテンツが暗号化されていれば、そのコピーもまた暗号化されており、そのコピー者は、そのコピー者が適切な復号化鍵を持っていない限りそのコンテンツへのアクセスを獲得することができない。セキュリティの維持が特に重要なオブジェクトについては、送信者および受信者のVDEノードによって制御される（以下に述べる）安全な通信技術を用いて、パーミッションレコード808および鍵ブロック810が頻繁に電子的に配布される。結果的に、パーミッションレコード808および鍵ブロック810は、好適な実施形態において、登録ユーザの電子機器600上にのみ頻繁に格納される（また、それら自身も登録／初期化プロセスの一部としてユーザに配送される）。この例においては、各プロパティのパーミッションレコード808および鍵ブロック810はSPU 500の安全なメモリ内にのみ格納される秘密DES鍵で暗号化して、鍵ブロックを他のいかなるユーザのVDEノードにも使用不可能にすることができる。あるいは、鍵ブロック810をエンドユーザの公開鍵で暗号化して、こららの鍵ブロックが対応する秘密鍵を格納しているSPU 500に対してしか使用できないようにすることができる（あるいは、他の許容可能な程度に安全な、暗号化／セキュリティ技術が使用できる）。

好適な実施形態においては、各パーミッションレコード808あるいは他の管理情報レコードを暗号化するために用いられる１つ以上の鍵は、レコードが更新さ

れる度に（あるいは、特定の１つ以上のイベントの後で）変更される。この場合、更新されたレコードは、新たな１つ以上の鍵を用いて再暗号化される。あるいは。管理情報を暗号化および復号化するのに用いられる１つ以上の鍵は、ある期間を経過すると自動的に無効になる「経時変化する」鍵であってもよい。経時変化鍵と他のイベント誘発(event triggered)鍵との組み合わせもまた望ましいものであり得る。例えば、特定回数のアクセス後および／または特定期間経過後あるいは絶対時刻に鍵に変化が生じるものであってもよい。所与の鍵あるいは鍵の組み合わせに対して、上記の技術を併用することも可能である。経時変化鍵を構築す

る好適な実施形態におけるプロシージャは、SPU RTC 528が提供するリアルタイム値の特定部分ならびにユーザおよびサイト情報を含む入力パラメータを用いた１方向旋回アルゴリズムである。例えば、ユーザあるいはサイト情報、絶対時刻、および／または、VDE安全コンテンツの使用／復号化若しくはVDEシステムの使用に関するアクティビティの部分集合に関連する期間のみを用いる技術等の、経時変化を生じさせるための他の技術を用いることも可能である。

VDE 100は、図17に示される論理オブジェクト構造800を有する多数の異なる種類の「オブジェクト」300をサポートする。ある意味において、オブジェクトは、プロテクション情報がプロテクトされる情報と結合しているかどうかによって分類され得る。例えば、その制御によって特定のVDEノードに結合されているコンテナは「静止オブジェクト」と呼ばれる（図18参照）。その制御情報によって特定のVDEノードに結合されておらず、数カ所のサイトにおける全体的なあるいは部分的な使用を可能にするのに十分な制御およびパーミッションを有しているコンテナは「移動オブジェクト」と呼ばれる（図19参照）。

また別の意味においては、オブジェクトは、そのオブジェクトが有する情報の性質によって分類され得る。情報コンテンツを有するコンテナは「コンテンツオブジェクト」と呼ばれる（図20参照）。取引情報、監査追跡、VDE構造および／または他のVDE制御／管理的情報を包含するコンテナは、「管理的オブジェクト」と呼ばれる（図21参照）。（VDE制御情報であることに対して）VDE制御下で動

作する、実行可能なコードを包含する一部のコンテナは、「スマートオブジェクト」と呼ばれる。スマートオブジェクトは、ユーザエージェントをサポートし、遠隔サイトにおけるその実行を制御する。そのコンテンツに関連する位置、種類およびアクセスメカニズムによるオブジェクトの他の分類も存在する。これは、上記した種類の組み合わせを含み得る。VDE 100によってサポートされるこれらのオブジェクトのいくつかを以下で説明する。図17に示されるデータブロック812の一部あるいはその全ては、「埋込み」コンテンツ、管理的、静止、移動および／または他のオブジェクトを含み得る。

１．静止オブジェクト

図18は、好適な実施形態によって提供される「静止オブジェクト」構造850の一例を示す。「静止オブジェクト」構造850は、その静止オブジェクトの１つ以上の部分を使用する明示的なパーミッションを受け取った特定のVDE電子機器／インストレーション(installation)でのみ使用するように意図されている。従って、静止オブジェクト構造850は、パーミッションレコード（PERC）808を有しておらず、このパーミッションレコードは別に（例えば、異なる時刻に、異なるパスを介して、および／または異なるパーティによって）、機器／インストレーション600に供給および／または配送される。一般的なPERC 808を多数の異なる静止オブジェクトとともに用いることが可能である。

図18に示されるように、公開ヘッダ802は好ましくは「平文」（即ち、暗号化されていない文）である。秘密ヘッダ804は好ましくは、多数の「秘密ヘッダ鍵」の少なくとも１つを用いて暗号化される。秘密ヘッダ804は好ましくは、公開ヘッダ802からの識別情報エレメントのコピーを１つ有しており、これにより、平文公開ヘッダ内の識別情報が不正改変された場合に、システムは、不正改変者が改変しようとしたものが何であるのかを正確に決定することができる。メソッド1000は、オブジェクトローカルメソッド、ロードモジュール、および／またはユーザデータエレメントの形式の「秘密ボディ」806と呼ばれるセクション内に含まれ得る。この秘密ボディ（メソッド）セクション806は、好ましくは、別個のパーミッションレコード808内に含まれる１つ以上の秘密ボディ鍵を用いて暗号

化される。データブロック812は、やはりパーミッションレコード808内に提供される１つ以上のコンテンツ鍵を用いて暗号化され得る（情報あるいは管理的）コンテンツを有する。

２．移動オブジェクト

図19は、好適な実施形態によって提供される「移動オブジェクト」構造860の一例を示す。移動オブジェクトは、それらがVDEノードに到達したときにそれらのコンテンツの少なくとも一部の少なくとも部分的な使用を可能にするのに十分な情報を持っているオブジェクトである。

秘密ヘッダ804内にパーミッションレコード（PERC）808を有していることを除けば、移動オブジェクト構造860は、図18に示される静止オブジェクト構造850と同じである。移動オブジェクト構造860内にPERC 808を有していることによって、（メソッド1000および包含されるPERC 808に従って）あらゆるVDE電子機器／参加者600において移動オブジェクトを使用することが可能になる。

「移動」オブジェクトは、「チャネル外」配布を特にサポートし得るクラスのVDEオブジェクト300である。従って、移動オブジェクトは鍵ブロック810を有し、ある電子機器600から他の電子機器にトランスポート（transportable）可能である。移動オブジェクトには非常に限定された使用に関連する予算が付随している場合があり、これにより、ユーザは、（コンピュータプログラム、ゲーム、あるいはデータベース等の）コンテンツを全体的あるいは部分的に使用して、ライセンスを取得するのか、さらにライセンスするのか、あるいはオブジェクトコンテンツを購入するのかを判断することができる。あるいは、移動オブジェクトPERC 808は、例えば、

(a) 将来のライセンシングあるいは購入のために以前に購入した権利あるいは貸し方を反映するとともに、少なくとも１種類以上のオブジェクトコンテンツの使用を可能にする予算、および／または、

(b) オブジェクトコンテンツの使用を可能にするためにローカルVDEノードにおいて格納および管理された残っている(available)貸し方を採用する(およびこれを借方に記入し得る)予算、および／または、

(c)，ローカルVDEノードへのレポート（さらに、任意に、情報交換所へのレポート）が要求される前の１つ以上の最大使用基準（maximum usage criteria)を反映するとともに、その後でリセットを行って、オリジナルの１つ以上の予算の中の１つ以上のさらなる使用および／または改変を可能にし得る予算、

を有する、あるいは、これを用いて予算レコードを参照することができる。

標準的なVDEオブジェクト300の場合のように、利用可能な予算を使いきった後にユーザがその移動オブジェクトを継続して使用しようとする場合、または、移動オブジェクト（あるいはそのコピー）が異なる電子機器に移動され、その新しい機器が、パーミッションレコード808によって要求される要件に対応する利用可能な貸し方予算を有していない場合、ユーザは、情報交換所サービスにコンタクトをとって付加的な予算を獲得するように要求される場合がある。

例えば、移動オブジェクトPERC 808は、要求される予算VDE1200あるいは利用可能であると認められるおよび／または利用可能になることが予想される予算オプションに対するリファレンスを有し得る。予算VDEは、消費者のVISA、MC、AMEX、またはオブジェクト独立型であり、且つ特定のあるいは複数クラスの移動オブジェクトコンテンツの使用に適用可能な他の「一般(generic)」予算（例えば、Blockbuster Videoレンタルであり得るあるクラスの移動オブジェクトからのあらゆる映画オブジェクト(movie object)）を参照し得る。予算VDE自身は、それと共に使用され得る１つ以上のクラスのオブジェクトを要求し得、あるオブジェクトは特定の１つ以上の一般予算を特に参照し得る。このような場合、典型的に、VDEプロバイダは、正しい参照を可能にするとともに課金処理および結果的な支払を可能にするような方法で情報を提供する。

機器が、一般に若しくは特定の１つ以上のユーザあるいはユーザクラスに対して、正しい予算あるいは予算の種類（例えば、VISA予算等の情報交換所から利用可能な十分な貸し方）を有する限り、または、その移動オブジェクト自身が十分な予算割当額(budget allowance)若しくは適切な承認を有する限り、移動オブジェクトは受信VDEノード電子機器600において使用できる（例えば、その移動オブジェクトが特定の１つ以上のインストレーション若しくはインストレーションク

ラスあるいはユーザ若しくはユーザクラスに対して使用可能であるという規定(stipulation)。但し、クラスは、安全なデータベース610に格納され予め定義されたクラス識別名(identifiers)によって表されるインストレーション若しくはユーザの特定の部分集合に対応)。移動オブジェクトを受け取った後、ユーザ(および／またはインストレーション)が適切な予算および／または承認を有していない場合、ユーザは、電子機器600によって(その移動オブジェクト内に格納された情報を用いて)、どの１つ以上のパーティに対してユーザがコンタクトをとり得るのかを知らされる。そのパーティは、(そこからユーザが所望のコンタクトを選択する)移動オブジェクトの情報交換所プロバイダの択一的なリストを構成し得る。

上記のように、移動オブジェクトは、「チャネル外に」オブジェクト300を配布することを可能にする。つまり、オブジェクトは、不許可のあるいは明示的には

許可されていない個人から別の個人に配布され得る。「チャネル外」は、例えばユーザがあるオブジェクトを別の個人に直接的に再配布することを可能にする配布経路(path of distribution)を含む。例えば、オブジェクトプロバイダは、ユーザがあるオブジェクトのコピーをそのユーザの友人若しくは同僚に(例えば、記憶媒体の物理的な配送、あるいは、コンピュータネットワーク上での配送によって)再配布することを可能にして、これにより、友人若しくは同僚がそのオブジェクトを使用するために要求される何らかの特定の基準を満たした場合にその友人若しくは同僚に使用を許可することが可能である。

例えば、ソフトウェアプログラムが移動オブジェクトとして配布された場合、そのプログラムのユーザが、そのソフトウェアあるいはそのソフトウェアの使用可能なコピーを友人に供給したいと願っている場合、通常は自由にそうすることができる。移動オブジェクトには、大きな商業的価値が秘められている。なぜなら、有用なコンテンツは主にユーザおよび電子掲示板によって配布され得、「オリジナル」コンテンツプロバイダおよび／または情報交換所への登録の他には配布オーバーヘッドがほとんどあるいは全く必要でないからである。

「チャネル外」配布は、プロバイダが、使用に対する支払を受け取ることおよび／または再配布されたオブジェクトの少なくともある程度の制御を別の方法で維持することをも可能にし得る。このような特定の基準は、例えば、その使用のために十分に利用可能な貸し方のあるクレジットカード等の承認されたサードパーティ金融関係のユーザVDEノードにおける登録された存在を含み得る。

従って、ユーザがVDEノードを持っていた場合、もしユーザが、ユーザのVDEノード上で利用可能な（また、必要な場合、ユーザに割り当てられた）適切な利用可能な予算を持っていたならば、および／または、もしユーザまたはユーザのVDEノードが、特別に承認されたグループのユーザ若しくはインストレーションに属していたならば、および／または、もし移動オブジェクトがそれ自身の予算を持っていたならば、そのユーザはその移動オブジェクトを使用することができるかもしれない。

移動オブジェクトのコンテンツは暗号化されており、そのオブジェクトに用いられている移動オブジェクト秘密ヘッダ鍵が破損していない限り、移動オブジェクトのコンテンツは、承認された状況下でのみ使用できる。これは、例えば、パーミッションおよび／または予算情報に比べた場合、移動オブジェクトの比較的容易なタスクであり得る。なぜなら、多数のオブジェクトが同一の鍵を共有しており、分析すべきよりたくさんの暗号文情報と暗号解析を行うより強い動機の両方を暗号解析者に与え得るからである。

「移動オブジェクト」の場合、コンテンツの所有者は、そのコンテンツがカプセル化されているオブジェクト300内に含まれている鍵ブロック810の一部あるいはその全てとともに情報を配布し得る。配布されるオブジェクト300内に鍵を置けば、秘密ヘッダの保護に用いられている暗号化アルゴリズムを破るあるいは暗号解析することによって（例えば、ヘッダの暗号化の鍵を決定することによって）セキュリティメカニズムを突破しようとする試みに曝される危険性が増大する。セキュリティの突破は通常、相当な技術と時間を要するが、もし突破された場合、そのアルゴリズムおよび鍵が公開されて、これと同一の鍵およびアルゴリズムによってプロテクトされているオブジェクトを持っている多数の個人がプロテ

クトされた情報を不正使用できるようになる。結果的に、配布されるオブジェクト300内に鍵を置くことは、「時間に左右される」（特定の期間経過後には値が減少している）あるいはその値が幾分制限されるコンテンツ、または、鍵をオブジェクト内に置く商業的価値（例えば、エンドユーザにとっての便利さ、遠距離通信あるいは鍵および／またはパーミッション情報を配送する他の手段および／または「チャネル外」に出ていくオブジェクトのサポートに対する能力を排除する比較的低いコスト）が、高度なハッカーに対する被攻撃性のコストを上回る場合に限定され得る。他の箇所で述べられているように、旋回技術を採用して移動オブジェクト内に「真性（true）」鍵を格納しないようにすることによって、鍵のセキュリティを高めることができるが、ほとんどの場合、サイトIDおよび／または時刻ではなくて、VDE管理者によってほとんどあるいは全てのVDEノードに入力として提供される共有のシークレット（shared secret）を用いることによってオブジェクトをこれらの値から独立した状態に維持する。

図19に示し、先に述べたように、移動オブジェクトは、好ましくは少なくとも何らかの予算（一般的な場合、一方、他方、あるいは両方）を提供するパーミッションレコード808を有する。上記のように、パーミッションレコード808は、重要な鍵情報を格納している鍵ブロックを有し得る。PERC 808は、有価数量（valuable quantities）／値（values）を有する可能性のある予算を持っているか、あるいはこれを参照し得る。このような予算は、移動オブジェクト自身の中に格納されるか、あるいは、別々に配送されて高度安全通信鍵および管理的オブジェクト鍵および管理データベース技術によって保護され得る。

移動オブジェクトに含まれるメソッド1000は、典型的に、オブジェクト内のパーミッションレコード808（例えば、REGISTERメソッド）を用いてそのオブジェクトを「自己登録」するためのインストレーションプロシージャを含む。これは、時間制限値を有するオブジェクトと、エンドユーザが料金を請求されないあるいは所定料金しか請求されないオブジェクト（あるいはプロパティ）（例えば、公開情報に実際にアクセスしたエンドユーザの数に基づいて広告主および／または情報発行者が料金請求されるオブジェクト）と、広く利用可能な予算を要求す

るとともにチャネル外配布から特に恩恵を受け得るオブジェクト（例えば、クレジットカードから派生する、映画、ソフトウェアプログラム、ゲーム等のプロパティを有するオブジェクトのための予算）とに特に有用であり得る。このような移動オブジェクトは、予算UDEを含んであるいは含まずに供給され得る。

移動オブジェクトの１つの使用方法であるソフトウェアの発行においては、顧客になる可能性のある者が、ライセンス料金を支払う前あるいは初期試用料金以上の料金を支払う前に、そのソフトウェアをデモンストレーションモードで使用する、あるいは可能であれば限られた期間内において完全なプログラム機能を使用することを、包含されるパーミッションレコードによって許可し得る。例えば、時間ベースの課金方法および小さな時間予算が予備インストールされた予算レコードを用いて、短い期間の間そのプログラムを完全に使用することを許可する。オブジェクトコンテンツの不正使用を回避するために様々な制御メソッドを用いることが可能である。例えば、移動オブジェクトの最小登録期間をある適切な長い期間（例えば、１ヶ月、６ヶ月あるいは１年間）に設定することによって、ユーザが同一の移動オブジェクト内の予算レコードを繰り返し使用することを防ぐことができる。

移動オブジェクトの使用を制御するもう１つの方法は、その移動オブジェクト内に組み込まれたパーミッションレコードに経時変化鍵を含めることである。これは、移動オブジェクトが、再登録を行うことなく特定日以降に使用されないようにするためのもので、一般に移動オブジェクトに有用であり、一斉通信、ネットワークあるいは（１方向および２方向ケーブルの両方を含む）遠距離通信によって電子的に配布される移動オブジェクトに特に有用である。なぜなら、このような移動オブジェクト経時変化鍵の配送の日付および時刻は、ユーザがそのオブジェクトの所有権を得た時刻に正確に対応するように設定できるからである。

移動オブジェクトを使用して、ある電子機器600から別の電子機器への「移動」を助長することも可能である。ユーザは、１つ以上のパーミッションレコード808が組み込まれた移動オブジェクトを、例えばデスクトップコンピュータから同じユーザのノートブックコンピュータへと移動させることができる。移動オブ

ジェクトがそのユーザをオブジェクト自身の中に登録して、その後はそのユーザしか使用できないようにすることが可能である。移動オブジェクトは、基本配布予算レコード用に１つ、および、登録ユーザの「アクティブ」配布予算レコード用のもう１つといった別々の予算情報を維持し得る。このようにすれば、オブジェクトをコピーしてユーザになり得る別の者に引き渡して、その後は、これを、そのユーザのためのポータブルオブジェクトとすることが可能である。

移動オブジェクトが他のオブジェクトを有するコンテナ内に入っている場合もある。例えば、移動オブジェクトコンテナは、コンテンツオブジェクトをエンドユーザオブジェクトレジストリ内に登録するため、および／または、パーミッションおよび／または他のセキュリティ機能を施行するためのメカニズムを提供するための、１つ以上のコンテンツオブジェクトおよび１つ以上の管理的オブジェクトを有し得る。包含された管理的オブジェクトを用いて必要なパーミッションレコードおよび／または予算情報をエンドユーザの電子機器内に設置（install）することが可能である。

コンテンツオブジェクト

図20は、VDEコンテンツオブジェクト構造880の一例を示す。コンテンツオブジェクト880は、概して、情報コンテンツを有するあるいは提供する。この「コンテンツ」は、任意の種類の電子情報であり得る。例えば、コンテンツには、コンピュータソフトウェア、映画、本、音楽、情報データベース、マルチメディア情報、バーチャルリアリティ情報、機械命令、コンピュータデータファイル、通信メッセージおよび／または信号、ならびに、少なくともその一部が１つ以上の電子機器によって使用あるいは操作される他の情報が含まれる。また、銀行間での取引、電子購入通信、ならびに、電子的に署名された契約書および他の法的な書類の送信、監査および秘密保護された商業記録等の電子商取引および通信について、これらの認証、制御および／または監査用にVDE 100を構成することも可能である。これらの取引に用いられる情報もまた、「コンテンツ」と呼ぶことができる。先に述べたように、このコンテンツは物理的にオブジェクトコンテナ内に格納される必要はなく、異なる時刻に別々に提供され得る（例えば、ケーブルに

よるリアルタイム供給）。

図20に示される特定の例におけるコンテンツオブジェクト構造880は、PERC 808を含んでいないので静止オブジェクトの一種である。この例の場合、コンテンツオブジェクト構造880は、そのコンテンツ812の少なくとも一部として、図5Aに示されるような埋込みコンテンツオブジェクト882を少なくとも１つ含んでいる。コンテンツオブジェクト構造880は、管理的オブジェクト870をも含み得る。従って、好適な実施形態によって提供されるオブジェクトは、１つ以上の「埋込み」オブジェクトを含み得る。

管理的オブジェクト

図21は、好適な実施形態によって提供される管理的オブジェクト構造870の一例を示す。「管理的オブジェクト」は、一般に、パーミッション、管理的制御情報、コンピュータソフトウェアおよび／またはVDE 100の動作に関連するメソッドを有する。使用レコード、および／またはVDE 100の動作において使用されるあるいはその動作に関連する他の情報を、さらにまたは択一的に有し得る。管理的オブジェクトは、例えばエンドユーザに対して開放されるVDEプロテクトされた「コンテンツ」が存在しないことによって、コンテンツオブジェクトからは区別できる。

オブジェクトが他のオブジェクトを有している場合もあるので、単一のオブジェクトが１つ以上のコンテンツを有するオブジェクトと１つ以上の管理的オブジェクトとを有する可能性もある。管理的オブジェクトを用いて、更新、使用報告、課金および／または制御の目的で、電子機器間での情報の送信を行うことができる。管理的オブジェクトは、VDE 100の管理およびVDE 100の正しい動作の維持を助長する情報を有する。一般に、管理的オブジェクトは、VDE情報交換所サービス、配布者、あるいはクライアント管理者およびエンドユーザの電子機器600等のVDEノードの２者の間で送信される。

この例における管理的オブジェクト構造870は、公開ヘッダ802と、秘密ヘッダ804（「PERC」808を含む）と、メソッド1000を有する「秘密ボディ」806とを含む。図20に示されるこの特定の例における管理的オブジェクト構造870は、PERC

808を有しているので移動オブジェクトの一種であるが、管理的オブジェクトからPERC 808を除外して静止オブジェクトとしてもよい。管理的オブジェクト構造870は、情報コンテンツを格納するのではなく、「管理的情報コンテンツ」872を格納する。管理的情報コンテンツ872は、例えば、それぞれ異なる「イベント」に対応する複数のレコード872a、872b、...872nを包含し得る。各レコード872a、872b、...872nは、「イベント」フィールド874を含み得るとともに、パラメータフィールド876および／またはデータフィールド878を任意に含み得る。これらの管理的コンテンツレコード872は、VDE 100によって、取引の途中に処理できるイベントを規定するために使用され得る。例えば、レコードを安全なデータベースに追加するように設計されたイベントは、その記録がどのようにして何処に格納されるべきかを示すパラメータ896、ならびに、追加すべきレコードを有するデータフィールド878を含み得る。別の例においては、購入、購入指示書、インボイス等の、管理的オブジェクトのクリエータと受取人との間の金融取引が、イベントの収集物によって表され得る。各イベントレコード872は、例えばエンドユーザの安全なデータベース610に追加あるいは変更を行うためにエンドユーザの電子機器600によって実行される命令セットであり得る。イベントは、例えば次のような多数の基本的な管理機能を行うことができる：関連するユーザ／グループレコード、権利レコード、パーミッションレコードおよび／またはメソッドレコードの提供を含む

オブジェクトレジストリへのオブジェクトの追加；（監査追跡情報を例えばより密な要約形式に「まとめる（rolling up）」ことによる、あるいは、実際に消去することによる）監査レコードの消去；以前に登録したオブジェクトのパーミッションレコード808の追加あるいは更新；予算レコードの追加あるいは更新；ユーザ権利レコードの追加あるいは更新；および、ロードモジュールの追加あるいは更新。

好適な実施形態において、管理的オブジェクトは、例えば、配布者、クライアント管理者、またおそらくは情報交換所若しくは他の金融サービスプロバイダからエンドユーザへと送信されるか、または例えばオブジェクトクリエータによっ

て配布者若しくはサービス情報交換所へと送信され得る。例えば、管理的オブジェクトは、管理的オブジェクトの送信先である受信VDEノードの予算および／またはパーミッションを増大あるいは調節し得る。同様に、イベントレコード872のデータ領域878内に監査情報を有する管理的オブジェクトは、エンドユーザから、配布者および／または情報交換所および／またはクライアント管理者へと送信され得る。配布者および／または情報交換所および／またはクライアント管理者は、それ自身も、オブジェクトクリエータあるいはオブジェクト処理連鎖の中の他の参加者への送信を行い得る。

メソッド

好適な実施形態におけるメソッド1000は、オブジェクトの使用および配布者との通信の際にユーザが出くわす処理の多くをサポートする。また、メソッド1000は、ユーザに対してどのメソッドフィールドが表示可能であるか（例えば、使用イベント、ユーザ要求イベント、ユーザレスポンスイベント、およびユーザ表示イベント）をも特定し得る。さらに、配布能力がそのメソッドにおいてサポートされている場合、そのメソッドは、配布アクティビティ、メソッドについてのユーザと配布者との通信、メソッド改変、配布者に対してどのメソッドフィールドが表示可能であるか、および、あらゆる配布データベースチェックおよび記録付け（例えば、配布イベント、配布者要求イベント、および配布者レスポンスイベント）をサポートし得る。

現存するメソッド構造の一般性、およびメソッドの組立に関する可能性の様々な配列(diverse array of possibilities)が与えられると、一般化された構成を用いてメソッド間の関係を確立することができる。メソッド1000は、あらゆる所与のセッションの間にそれらのメソッドを要求するオブジェクトから独立している場合があるので、それらのメソッド自身の中での関係を規定することは不可能である。好適な実施形態においては、「制御メソッド」を用いてメソッド間の関係を規定している。制御メソッドは、オブジェクト特異的であり得るとともに、各セッションにおける個々のオブジェクトの要件に対処し得る。

オブジェクトの制御メソッドは、他のメソッド間の関係を確立する。これらの

関係は、要求されるメソッド各々の所望のメソッドオプションを反映したレコードセットを登録プロセスにおいて構築する際に、明示的なメソッド識別名を用いてパラメータ化される。

好適な実施形態における「集合メソッド(aggregate method)」は、単一ユニットとして扱われ得るメソッドの収集物を表す。例えば、特定のプロパティに関するメソッドの収集物は、１つの集合メソッド内に格納され得る。この種の集合化(aggregation)は、実施の観点から見て有用であり得る。なぜなら、これは、記帳のオーバーヘッドを軽減するとともにデータベース全体の効率を向上させ得るからである。その他の場合、メソッドは、論理的に結合している(coupled)がゆえに集合化され得る。例えば、２つの予算は、その予算の一方が全体の制限を表し、第２の予算が使用について現在利用可能な制限を表すために、リンクされ(linked)得る。これは、例えば大きな予算が短い超過時間(over time)で開放された場合に起こり得る。

例えば、３つの別々のメソッドを用いる代わりに、計量、課金および予算プロセスを含んだ１つの集合メソッドを用いることが可能である。このような集合メソッドは、３つの別々のロードモジュールの機能を全てを行い且つ計量、課金および予算データを含んだ唯一のユーザデータエレメントを用いる単一の「ロードモジュール」1100を参照し得る。３つの別々のメソッドの代わりに１つの集合メソッドを用いることによって、全メモリ要件、データベースサーチ、復号化、および安全なデータベース610へのユーザデータエレメント書込の回数が最小限に

抑えられ得る。３つの別々のメソッドの代わりに１つの集合メソッドを用いることの欠点は、プロバイダおよびユーザ側の柔軟性が幾分損なわれることである。なぜなら、様々な機能を個別に交換することはもはや不可能だからである。

図16は、安全なデータベース610の一部としてのメソッド1000を示す。

基本命令および基本命令に関する情報の収集物である、好適な実施形態による「メソッド」1000は、１つ以上の電子機器600の動作に関する基本命令を行うおよび／または行う準備をする際に用いるコンテキスト、データ、要件および／または関係を提供するものである。図16に示されるように、好適な実施形態におけ

るメソッド1000は、安全なデータベース610内において、

C　メソッド「コア」1000N、

C　メソッドデータエレメント（MDE）1202、

C　ユーザデータエレメント（UDE）1200、および

C　データ記述(Description)エレメント(DTD)、

によって表される。

好適な実施形態におけるメソッド「コア」1000Nは、MDE 1202およびUDE 1200等の1つ以上のデータエレメントを包含あるいは参照し得る。好適な実施形態において、MDE 1202およびUDE 1200は同一の一般特性を有し得る。これら2種類のデータエレメント間の主な差異は、UDEは好ましくは特定のメソッドならびに特定のユーザあるいはユーザグループに結びつけら、一方、MDEは特定のメソッドに結びつけられ得るがユーザ独立型であり得ることである。好適な実施形態において、これらのMDEおよびUDEデータ構造1200および1202は、メソッド1000に入力データを提供するため、メソッドによって出力されるデータを受信するため、あるいはその両方のために使用される。MDE 1202およびUDE 1200を、これらを参照するメソッドコア1000Nから独立して配送するか、あるいは、データ構造をメソッドコアの一部として配送することが可能である。例えば、好適な実施形態におけるメソッドコア1000Nは、1つ以上のMDE 1202および／またはUDE 1200（あるいはその一部）を有し得る。メソッドコア1000Nは、それらを参照するメソッドコアから独立して配送される1つ以上のMDEおよび／またはUDEデータ構造を、択一的あるいは付加的に参照し得る。

好適な実施形態におけるメソッドコア1000Nは、1つ以上の「ロードモジュール」1100をも参照する。好適な実施形態におけるロードモジュール1100は、実行可能コードを包含し得るとともに、「データディスクリプタ」（「DTD」）情報と呼ばれる1つ以上のデータ構造をも包含あるいは参照し得る。この「データディスクリプタ」情報は、例えば、データ入力情報をDTDインタプリタ590に提供し得る。DTDは、ロードモジュール1100によるMDEおよび／またはUDEデータエレメント1202および1200へのアクセス（例えば、読み出しおよび／または書込み）を

可能にし得る。

メソッドコア1000'は、電子契約書の一部として含めるのに適したテキスト形式によるその動作の記述を有する１つ以上のDTDおよび／またはMDEデータ構造をも参照し得る。DTDおよびMDEデータ構造への参照は、メソッドコア1000'の秘密ヘッダ内で行われてもよいし、あるいは、以下に説明するイベントテーブルの一部として特定されてもよい。

図22は、好適な実施形態によって提供されるメソッドコア1000N用のフォーマットの一例を示す。好適な実施形態におけるメソッドコア1000Nは、メソッドイベントテーブル1006およびメソッドローカルデータ領域1008を有する。メソッドイベントテーブル1006は「イベント」を列記する。これらの各「イベント」は、あるイベントの処理を制御する「ロードモジュール」1100および／またはPERC 808を参照する。上記リスト内の各イベントには、そのイベントをサポートするのに必要なロードモジュール1000あるいはパーミッションレコード808ならびにメソッドユーザデータ領域1008へのリファレンスをパラメータ化するのに必要なあらゆる統計的データが関連付けられる。ロードモジュール1100をパラメータ化するデータは、部分的に、そのロードモジュールに対する特定の機能コールと考えることができ、また、それに対応するデータエレメントはその特定の機能コールのための入力および／または出力データと考えることができる。

メソッドコア1000Nは、単一のユーザに特異的であってもよく、あるいは、（例えば、そのメソッドコアおよび／または特定のユーザデータエレメントの固有性に依存して）複数のユーザ間て共有されていてもよい。具体的には、各ユーザ／グループが独自のUDE 1200を有し、共有メソッドコア1000Nを使用することが可能

である。この構成により、メソッドコア1000N全体を１つのユーザ／グループに関連付ける場合に比べて、データベースオーバーヘッドを削減することが可能になる。あるユーザがあるメソッドを使用することを可能にするために、そのユーザには、UDE 1200を特定するメソッドコア1000Nが送信され得る。そのメソッドコア1000Nがサイトの安全なデータベース610内に既に存在する場合、追加する必

要があるのはUDE 1200のみであり得る。あるいは、メソッドは、登録時刻において要求されるあらゆるUDE 1200を生成し得る。

好適な実施形態によって提供されるメソッドコア1000Nの図22に示される例は、公開（暗号化されていない）ヘッダ802、秘密（暗号化された）ヘッダ804、メソッドイベントテーブル1006、およびメソッドローカルデータ領域1008を含む。

メソッドコア1000N公開ヘッダ802の可能なフィールドレイアウトの一例を以下のテーブルに示す。

フィールドの種類		説明
メソッドID	クリエータID	このメソッドのクリエータのサイトID。
	配布者ID	このメソッドの配布者（例えば、最後の変更）。
	種類ID	メソッドの「種類」を表す一定値。
	メソッドID	このメソッドの固有のシーケンス番号。
	バージョンID	このメソッドのバージョン番号。
その他の分類情報	クラスID	異なるメソッド「クラス」をサポートするID
	種類ID	メソッドタイプ互換的サーチ(method type compatible searching)をサポートするID。
記述的情報(Descriptive Information)	記述	このメソッドのテキスト形式による記述。
	イベント要約	このメソッドがサポートするイベントクラス（例えば、USE）の要約。

秘密ヘッダ804の可能なフィールドレイアウトの一例を以下に示す。

フィールドの種類		説明
公開ヘッダ802メソッドIDおよび「その他の分類情報」のコピー		公開ヘッダにあるメソッドID。
記述的情報	イベントの数	このメソッドにおいてサポートされるイベントの数。
アクセスおよび参照タグ	アクセスタグ	このメソッドがSPUによる管理下において正しいメソッドであるかどうかを判定するため、即ち、メソッドコア1000Nが適切な状況下においてのみ使用されていることを確実にするために使用されるタグ。
	有効性検査タグ	
	相関タグ	
データ構造リファレンス		DTDおよび／またはMDEに対する任意に省略可能なリファレンス。
チェック値		秘密ヘッダおよびメソッドイベントテーブルのチェック値。
公開ヘッダのチェック値		公開ヘッダのチェック値。

図２２を再び参照して、好適な実施態様におけるメソッドイベントテーブル1006は、１～Ｎメソッドイベントレコード1012を有していてもよい。これらメソッドイベントレコード1012の各々は、メソッドコア1000Nによって表されるメソッド1000が応答し得る、異なるイベントに対応する。好適な実施態様におけるメソッド1000は、その応答するイベントに依存して全く異なる振る舞いをし得る。例えば、AUDITメソッドは、ユーザによるオブジェクトその他のリソースの使用に対応するイベントに応答して、監査追跡UDE1200に情報を格納し得る。この同じAUDITメソッドは、管理イベント、例えばVDEノード内においてタイマーが切れることや他のVDE参加者からの監査追跡の報告の要求(request)等に応答して、格納された監査追跡をVDE管理者またはその他の参加者に対して報告し得る。好適な実施態様において、これらの異なるイベントの各々を「イベントコード」によって表すことができる。この「イベントコード」は、メソッドがコールされたときにパラメータとしてメソッドに渡され、メソッドイベントテーブル1006中の適切

なメソッドイベントレコード1012を「ルックアップ」するために用いられ得る。選択されたメソッドイベントレコード1012は次に、起こったイベントに応答して実行されるコンポーネントアセンブリ690を構築するために用いられる適切な情報（例えばロードモジュール1100、データエレメントUDEおよびMDE1200、1202および／またはPERC808）を指定する（specify）。

従って、好適な実施態様において、各メソッドイベントレコード1012は、イベントフィールド1014、LM/PERCリファレンスフィールド1016、および任意の数のデータリファレンスフィールド1018を有し得る。好適な実施態様においてイベントフィールド1014は、対応イベントを識別する「イベントコード」またはその他の情報を含んでいてもよい。LM/PERCリファレンスフィールド1016は、ロードされて実行されることによってイベントに応答してメソッドを実行する実行可能コードを提供（または参照）する、ロードモジュール1100および／またはPERC808を識別する、安全データベース（secure database）610へのリファレンス（またはその他の「ポインタ」情報）を提供し得る。データリファレンスフィールド1018は、UDE1200またはMDE1202を参照する情報を含み得る。これらのデータ構造は、メソッドコア1000Nのメソッドローカルデータ領域1008中に含まれていてもよく

または安全データベース610中に独立のデリバラブル（deliverables）として格納されてもよい。

以下のテーブルは、メソッドイベントレコード1012のより詳細なフィールドレイアウトの可能性例である：

フィールドタイプ		説明
イベントフィールド1014		対応するイベントを識別する。
アクセスタグ		メソッドイベントレコードのこの行にアクセスを許可する秘密のタグ。
LM/PERC リファレンスフィールド1016	DB ID またはオフセット／サイズ	データベースリファレンス（またはローカルポインタ）。
	コリレーションタグ	このエレメントを参照するときにアサートするコリレーションタグ。
データエレメントリファレンスフィールドの数		メソッドイベントレコード中のデータリファレンスフィールドのカウント。
データリファレンスフィールド1	UDE IDまたはオフセット／サイズ	データベース610リファレンス（またはローカルポインタ）。
	コリレーションタグ	このエレメントを参照するときにアサートするコリレーションタグ。
!	...	
データリファレンスフィールドn	UDE IDまたはオフセット／サイズ	データベース610リファレンス（またはローカルポインタ）。
	コリレーションタグ	このエレメントを参照するときにアサートするコリレーションタグ。

ロードモジュール

図２３は、好適な実施態様において提供されるロードモジュール1100の例を示す。一般に、ロードモジュール1100は、制御動作に用いられる基本機能群を表す。

ロードモジュール1100は、コードおよびスタティックデータ（機能的にコードと同等なもの）を含んでおり、VDE100の基本動作を行うために用いられる。ロードモジュール1100は一般に、システム中の全オブジェクトのための全ての制御構造によって共有されるが、専有(proprietary)ロードモジュールもまた許容される。ロードモジュール1100は、管理オブジェクト構造870内においてVDE参加者間で受け渡しされ、通常は安全データベース610内に格納される。これらは常に暗

号化されており、これら両ケースにおいて認証(authenticate)される。メソッドコア1000Nがロードモジュール1100を参照するとき、ロードモジュールはSPE503にロードされ、復号化され、電子機器のマイクロプロセッサに渡されてHPE655内で実行されるか（そこが実行場所であれば）、またはSPE内に保持される（そこが実行場所であれば）。SPE503が存在しなければ、ロードモジュールは、実行以前にHPE655によって復号化される。

パーティによるロードモジュール作成は、好ましくは証明プロセスまたはリング型SPUアーキテクチャで制御される。このようにして、すでに安全化データベース610に格納されているロードモジュールのリプレース(replace)、更新、または削除するプロセスもそうであるように、新しいロードモジュール1100を作成するプロセス自体もまた、制御されたプロセスとなる。

ロードモジュール1100は、SPE503またはHPE655の保護された環境内で実行されたときのみ、その機能を果たすことができる。なぜなら、その場合においてのみ、ロードモジュール1100が動作する対象である保護されたエレメント（例えば、UDE1200、他のロードモジュール1100）へアクセスすることが可能になるからである。この環境におけるロードモジュールの実行の開始は、アクセスタグ、有効性検査タグ、暗号化鍵、デジタル署名、および／またはコリレーションタグの組み合わせによって厳しく制御される。このようにして、ロードモジュール1100は、発信者(caller)がそのIDを知っていてそのロードモジュールに特異的な共有された秘密のコリレーションタグをアサートした場合にのみ、参照され得る。復号化SPUは、復号化後に、ロードモジュールのローカルアクセスタグと識別トークンとをマッチしてもよい。これらの技術は、いかなるロードモジュール1100の物理的なリプレースをも、ロードモジュールの次の物理的なアクセス時において、検

知可能にする。さらに、好適な実施態様において、ロードモジュール1100は「リードオンリー」にされてもよい。ロードモジュール1100を「リードオンリー」属性にすることにより、安全でない空間で不正改変されたロードモジュールによる書き換えが防がれる。

ロードモジュールは、これらを制御するPERC808によって直接支配される必要はなく、また、時刻／日付情報または失効日(expiration date)を含んでいる必要もない。好適な実施態様における唯一の制御上の考慮は、一つ以上のメソッド1000がコリレーションタグ（ロードモジュールのオーナーによって作成された保護されたオブジェクトの値、承認されたパーティに対して彼らのメソッドに含めるために配布され、そのアクセスおよび使用は一つ以上のPERC808によって制御される）を用いてこれらを参照することである。もしメソッドコア1000Nがロードモジュール1100を参照して正しいコリレーションタグをアサートすれば（そしてロードモジュールがSPE503の内部不正改変チェックを満足すれば）、ロードモジュールはロードし実行されることが可能になり、あるいは他のシステムから入手されるか、他のシステムに送られるか、他のシステムによって更新されるか削除されることが可能になる。

図２３に示すように、好適な実施態様におけるロードモジュール1100は、公開（非暗号化）ヘッダ802、秘密（暗号化）ヘッダ804、暗号化された実行可能コードを含む秘密本体1106、および一つ以上のデータ記述エレメント（DTD）1108から構成され得る。DTD1108は、ロードモジュール1100に格納されてもよく、あるいは、安全データベース610中のスタティックデータエレメントへのリファレンスであってもよい。

以下は、ロードモジュール公開ヘッダ802のフィールドレイアウトの可能性例である：

フィールドタイプ		説明
LM ID		ロードモジュールのVDE ID。
	作成者ID	このロードモジュールの作成者のサイトID。
	タイプID	ロードモジュールタイプを示す定数。
	LM ID	このロードモジュールに対するユニークなシーケンスナンバー。承認されたVDE参加者によって作成されたロードモジュールのシーケンス中のロードモジュールをユニークに識別する。
	バージョンID	このロードモジュールのバージョンナンバー。
他の分類情報	クラスID	ロードモジュールの異なるクラスをサポートするためのID。
	タイプID	メソッドタイプ互換性サーチをサポートするためのID。
記述的情報	記述	ロードモジュールのテキスト記述。

	実行空間コード	このロードモジュールはどの実行空間であるか（例えばSPEまたはHPE）を記述する値。

多くのロードモジュール1100は、SPE503で実行するコードを含んでいる。HPE655で実行するコードを含んでいるロードモジュール1100もある。このことは、メソッド1000がどちらでも適切な方の環境で実行することを可能にする。例えば、INFORMATIONメソッド1000は、政府クラスの安全性のためSPE503安全空間中のみで実行するように構築されるか、あるいは商業アプリケーションのためにHPE655中でのみ実行するように構築され得る。上述のように、公開ヘッダ802は、ロードモジュール1100をどこで実行する必要があるかを示す「実行空間コード」フィールドを含んでいてもよい。この機能性は、異なるユーザプラットホームだけでなく、異なるSPE命令セットを可能にし、その基礎となるロードモジュール命令セットに依存することなくメソッドを構築することを可能にする。

ロードモジュール1,100は、３つの主要データ領域上で動作する。すなわち、スタック、ロードモジュールパラメータ、およびデータ構造である。ロードモジュール1100を実行するために必要なスタックおよび実行メモリサイズは好ましくは、ロードモジュールコール、リターン時のスタックイメージおよび任意のリターンデータ領域からのデータ記述と同様、秘密ヘッダ804に記述されている。スタックおよびダイナミック領域は、同じDTDメカニズムを用いて記述される。以下は、ロードモジュール秘密ヘッダ1104のフィールドレイアウトの可能性例である：

フィールドタイプ		説明
公開ヘッダ802からの情報の一部または全部のコピー		公開ヘッダからのオブジェクトID。
他の分類情報	チェック値	公開ヘッダのチェック値。
記述的情報	LMサイズ	実行可能コードブロックのサイズ。
	LM実行サイズ	ロードモジュールの実行可能コードサイズ。
	LM実行スタック	ロードモジュールに必要なスタックサイズ。
	実行空間コード	このロードモジュールの実行空間を記述するコード。
アクセスおよびリファレンスタグ	アクセスタグ	ロードモジュールがSPEによって要求された正しいLMであるか否かを決定するために用いられるタグ。
	有効性検査タグ	
	コリレーションタグ	発信者がこのLMを実行する権利を有するか否かを決定するために用いられるタグ。
	デジタル署名	LM実行可能が不正改変されていず、信頼できるソース（LMを作成するための正しい証明書を有するソース）によって作成されたか否かを決定するために用いられる。
データレコードデスクリプタ情報	DTDカウント	コードブロックに続くDTDの数
	DTD１リファレンス	ローカルに定義されている場合、このLMについて定義された第１番目のDTDの物理サイズおよびバイト単位のオフセット。 パブリックに参照されるDTDの場合、これがDTD IDかつレコードへのアクセスを許可するためのコリレーションタグである。

	DTD Ｎリファレンス	ローカルに定義されている場合、このLMについて定義された第Ｎ番目のDTDの物理サイズおよびバイト単位のオフセット。 パブリックに参照されるDTDの場合、これがDTD IDかつレコードへのアクセスを許可するためのコリレーションタグである。
チェック値		LM全体のチェック値。

各ロードモジュール1100はまた、ロードモジュールからメソッドを構築するこ

とをサポートするために必要な情報を提供するために、DTD1108情報を用いてもよい。このDTD情報は、ロードモジュールがサポートする全てのメソッドデータフィールドの名前およびデータタイプの、SGML等の言語で表現された定義および、フィールドに置くことのできる値の容認可能範囲を含む。他のDTDは、例えば、電子契約へ含めるため用にロードモジュール1100の機能を英語で記述してもよい。

ロードモジュール1100の次のセクションは、一つ以上の暗号化コードブロックを含む、暗号化された実行可能本体1106である。ロードモジュール1100は好ましくは、効率およびコンパクトさのため、その実行環境における「ネイティブ」命令セットでコードされる。SPU500およびプラットホームプロバイダは、その製品をVDE100で考えられている配布メカニズムのコンテンツと協力(cooperate)できるように、標準ロードモジュール1100の様々なバージョンを提供してもよい。好適な実施態様では、有限リソースSPUの性能を最適化するために、インタープリトされたあるいは「ｐ－コード」ソリーションではなく、ネイティブモードロードモジュール1100を作成し使用する。しかし、十分なSPE（またはHPE）リソースが存在するときおよび／またはプラットホームが十分なリソースを有するときは、これら他のインプリメンテーションアプローチにより、ロードモジュールコードのクロスプラットホーム的有用性が改善される。

以下は、ロードモジュールDTD1108のフィールドレイアウト例である：

フィールドタイプ		説明
DTD ID		秘密ヘッダからのオブジェクトIDを用いる。

	作成者ID	このDTDの作成者のサイトID。
	タイプID	定数。
	DTD ID	このDTDのユニークなシーケンスナンバー。
	バージョンID	このDTDのバージョンナンバー。
記述的情報	DTDサイズ	DTDブロックのサイズ。
アクセスおよびリファレンスタグ	アクセスタグ	このDTDがSPEによって要求された正しいDTDであるか否かを決定するために用いられるタグ。
	有効性検査タグ	
	コリレーションタグ	このDTDの発信者がDTDを実行する権利を有するか否かを決定するために用いられるタグ。
DTD本体	DTDデータ定義１	
	DTDデータ定義２	
	!	
	DTDデータ定義N	
	チェック値	DTDレコード全体のチェック値。

ロードモジュール1100がDTD1108を使用し得る方法の一例：

C　データ領域DTD4中のデータエレメント（DTD3内の名前により定義される）の値をDTD1中の値だけインクリメントする

C　データ領域DTD4中のデータエレメント（DTD3内の名前により定義される）の値をDTD3中の値にセットする

C　DTD3中のテーブルからのDTD1中のイベントからの原子エレメントを計算してDTD2内にリターンする

C　DTD3中の等式からのDTD1中のイベントからの原子エレメントを計算してDTD2内にリターンする

C　DTD3中で参照されたロードモジュール作成テンプレートからロードモジュールを作成する

C　DTD4内のコンテンツを用いてDTD3内のロードモジュールを改変する

Ｃ　ＤＴＤ3内に名前があるロードモジュールを破棄(destroy)する

スペースが許す限り、共通に用いられるロードモジュール1100をSPU500中にビルドインしてもよい。ビルトインのロードモジュール1100を用いるVDEプロセスは、外部ロードモジュールを見つけ、ロードして復号化しなければならないプロセスよりも大きく改善されたパフォーマンスを示す。SPU内にビルドインされ得るロードモジュール1100で最も有用なものは、スケーラ計量(scaler meter)、固定価格課金、予算およびこれらの３つのプロセスを行う混合メソッド(aggregate method)のためのロードモジュールなどである。

ユーザデータエレメント（UDE）1200およびメソッドデータエレメント(MDE)1202

好適な実施態様におけるユーザデータエレメント（UDE）1200およびメソッドデータエレメント(MDE)1202は、データを格納する。好適な実施態様で提供されるUDE1200およびMDE1202には、多くのタイプがある。好適な実施態様において、これら異なるタイプのデータ構造の各々は、共通ヘッダ定義および名前付けスキームを含む、共通の全体フォーマットを共有する。この共通構造を共有する他のUDE1200は、「ローカルネームサービスレコード」（すぐ下に説明する）および他のVDE参加者に接続するためのアカウント情報を含む。これらのエレメントは

必ずしも個々のユーザに関連付けられていず、従ってMDE1202と見なされてもよい。好適な実施態様で提供される全てのUDE1200および全てのMDE1202は、所望であれば（図16に示すように）、安全データベース610内の共通の物理テーブル内に格納されてもよく、データベースアクセスプロセスは、これらの異なるタイプのデータ構造の全てへのアクセスのために共通に用いられてもよい。

好適な実施態様において、PERC808およびユーザ権利テーブルレコードは、UDE1200のタイプである。他にも多くのタイプのUDE1200／MDE1202があり、例えば、計量、計量追跡、予算、予算追跡、および監査追跡がこれに含まれる。これら異なるタイプのUDE／MDEのための異なるフォーマットが、上述のように、DTD1108中に含まれるSGML定義によって定義される。メソッド1000は、適切にUDE／MDE1200、1202にアクセスするためにこれらのDTDを用いる。

安全データベース610は、２つのタイプのアイテムを格納する。すなわちスタティックとダイナミックである。スタティックデータ構造およびその他のアイテムは、実質的にスタティックな情報のために用いられる。これは、ロードモジュール1100、PERC808およびメソッドの多くのコンポーネントを含む。これらのアイテムは頻繁には更新されず、情報の「古い」コピーが新しく受け取られたアイテムによって置換される(substitute)ことを防ぐために用いることができる失効日、を含んでいる。これらのアイテムは、安全データベース610に格納される際に、サイト特異的な安全データベースファイル鍵を用いて暗号化され、SPEにロードされる際にその鍵を用いて復号化されてもよい。

ダイナミックアイテムは、頻繁に更新されなければならない安全なアイテムをサポートするために用いられる。多くのメソッドのUDE1200は、各使用後に、更新されSPE503から書き出されなければならない(written out)。計量および予算は、この通常例である。失効日は、予算UDE1200の以前のコピーによる置き換えを防ぐためには効果的に用いられ得ない。これらの頻繁に更新されるアイテムを安全にするためには、取引タグが発生され、そのアイテムが更新される度毎に暗号化されたアイテムに含められる。全てのVDEアイテムIDのリストおよび各アイテムの現在の取引タグは、安全データベース610の一部として維持される。

図２４は、好適な実施態様で提供されるユーザデータエレメント（UDE）1200の一例である。図２４に示すように、好適な実施態様におけるUDE1200は公開ヘッダ802、秘密ヘッダ804、およびデータ領域1206を有している。これらユーザデータエレメント1200の各々のレイアウトは一般に、UDE1200上で動作する一つ以上のロードモジュール1100に関連するDTD1108内に含まれるSGMLデータ定義によって定義される。

UDE1200は好ましくは、いったんサイトにロードされるとサイト特異的な鍵を用いて暗号化される。SPE503によって暗号学的に強い疑似ランダムシーケンス(pseudo-random sequence)から得られ得、レコードが安全データベース610に書き戻される度毎に更新され得る有効性検査タグを、このサイト特異的な鍵はマスクする。この技術は、UDE1200が、次回の使用時にシステムに要求されたときに、

不正改変されたり置き換えられたりしていないことの適度な(reasonable)保証を提供する。

計量および予算は、おそらくVDE100中において最も普通に見られるデータ構造である。これらは、イベントをカウントおよび記録するため、またイベントを制限するために用いられる。各計量および予算のためのデータ構造は、情報を変更することを承認されたコンテンツプロバイダまたは配布者／再配布者によって決定される。しかし、計量および予算は一般に、共通ヘッダフォーマットで格納された共通情報（例えばユーザID、サイトIDおよび関連の識別情報）を有している。

コンテンツプロバイダまたは配布者／再配布者は、各計量および予算UDEに対してデータ構造を指定し得る。これらのデータ構造は特定のアプリケーションに依存して変化し得るが、共通性の高いものもある。以下のテーブルに、METERおよびBUDGETメソッドにおける共通性の高いデータ構造の一部を挙げる：

フィールドタイプ	フォーマット	典型的な使用法	説明または使用法
昇順使用カウンタ	バイト、短、長、または同じ幅の無符号バージョン	計量／予算	使用の昇順カウント。
降順使用カウンタ	バイト、短、長、または同じ幅の無符号バージョン	予算	許可された使用の降順カウント。例えば残予算。

カウンタ／リミット	２、４または８バイトの整数が２つの関連するバイトまたはワードに分割されたもの	計量／予算	特定の時刻からの使用リミット。一般に複合計量(compound meter)データ構造に用いられる。
ビットマップ	アレイバイト	計量／予算	使用または所有権のビットインジケータ。
ワイドビットマップ	バイトアレイ	計量／予算	時とともに加齢し得る使用または所有権のビットインジケータ。
最終使用日	time_t	計量／予算	最終使用日
開始日	time_t	予算	最初の使用可能日
失効日	time_t	計量／予算	失効日
最終監査日	time_t	計量／予算	最終監査日
次監査日	time_t	計量／予算	次に必要な監査日
監査役	VDE ID	計量／予算	承認された監査役のVDE ID

上記テーブル中の情報は、完全あるいは包括的ではなく、計量および予算関連のデータ構造中に格納され得るタイプの情報の数例を示すことを意図している。特定の計量および予算の実際の構造は、そのデータ構造を作成し操作(manipulate)するロードモジュール1100に関連する一つ以上のDTD1108によって決定される。VDE100中のDTDインタプリタ590によって許可されたデータタイプのリストは、正しく承認されたパーティには利用可能(extensible)である。

図２５は、特に有利な種類のUDE1200データ領域1206の一例を示す。このデータ領域1206は、使用(usage)情報を記録するために用いられ得る「マップ」を定義する。例えば、計量メソッド1000は、一つ以上の「ユーセージマップ(usage m

ap)」データ領域1206を維持してもよい。ユーセージマップは、数タイプまたはカテゴリーの使用の各々に対応する、1ビット以上の情報（すなわち単次元または多次元ビットイメージ）を格納するという意味において、「使用ビットマップ」であり得る。ユーセージマップは、以前の使用を参照するための効率的な手段である。例えば、ユーセージマップデータ領域は、ユーザが使用するために支払いを行った情報コンテンツの全ての該当部分を、計量メソッド1000が記録するために用いられ得、このことにより情報コンテンツの同じ部分を後にユーザが使用することを可能にするための、非常に効率的かつ柔軟な手段をサポートする。これは、「連続性(contiguousness)」、「論理的関連性」、「使用のランダム化」および他の使用タイプなどの、ある種のVDE関連セキュリティ機能を、可能にし得る。ユーセージマップは、他の使用パターン（例えば、量ディスカウンティング、すなわちあるユーザが過去に無制限使用のために支払いを行った対象である情報コンテンツに再アクセスすることを可能にする）についても分析され得る。

好適な実施態様の提供する「ユーセージマップ」コンセプトは、「原子エレメント」のコンセプトに結びつけることができる。好適な実施態様において、オブジェクト300の使用は、「原子エレメント」単位で計量し得る(meter)。好適な実施態様において、計量文脈における「原子エレメント」とは、計量に記録されるのに「十分有意である」使用の単位を定義する。何をもって「原子エレメント」とするのかの定義は、オブジェクト300の作成者によって決定される。例えば、オブジェクト300に含まれる情報コンテンツの1「バイト」を「原子エレメント」と定義してもよく、または、データベースの1レコードを「原子エレメント」と定義してもよく、または、電子出版された本の各章を「原子エレメント」と定義してもよい。

オブジェクト300は、互いに重なる複数の原子エレメントのセットを有していてもよい。例えば複数のデータベース中の任意のデータベースへのアクセスを、原子エレメントと定義してもよい。同時に、任意のレコード、レコードのフィールド、情報のセクタ、および／または複数のデータベースのうち任意のものに含まれるバイトへのアクセスもまた、「原子エレメント」と定義され得る。電子出

版された新聞の場合、１つの記事の100ワード毎を「原子エレメント」と定義する一方、ある長さ以上の記事を別の「原子エレメント」のセットと定義してもよい。新聞中のある部分（例えば公告、求人欄など）は原子エレメントにマップされないかもしれない。

好適な実施態様は、原子エレメントタイプの定義に関して、オブジェクトの作成者にとって実質的に無制限の能力を提供する。このような原子エレメントの定義は、様々な異なるコンテンツ使用を包含するように、非常に柔軟にされ得る。好適な実施態様でサポートされる原子エレメントタイプの例として、バイト、レコード、ファイル、セクタ、オブジェクト、一定量のバイト、連続的または相対的に連続的な(relatively contiguous)バイト（または他の予め定義された単位タイプ）、トピック、場所またはユーザ指定可能なその他の論理関係による、何らかの論理的関係を含む論理的に関連したバイト等がある。コンテンツ作成者は好ましくは、柔軟に他のタイプの原子エレメントを定義し得る。

本発明の好適な実施態様は、使用イベントと原子エレメントとの間のマッピングを提供するために、EVENTメソッドを提供する。一般に、オブジェクト300について定義される原子エレメントの異なるセットの各々に対して一つのEVENTメソッドがあり得る。多くの場合において、オブジェクト300は、課金に関連した計量のための少なくとも一つのタイプの原子エレメントおよび、非課金関連の計量のための少なくとも別の一つのタイプの原子エレメント（例えば、詐欺を検知したり、広告者に課金したり、および／またはエンドユーザの行動に関するデータを収集したりするために用いられる）を有するであろう。

好適な実施態様において、使用関連文脈における各EVENTメソッドは、２つの機能を果たす：（１）アクセスされたイベントをゼロ以上の原子エレメントのセットにマップすること、および（２）オブジェクト使用を計量するための一つ以上のMETERメソッドに情報を提供することである。このアクセスイベントと原子エレメントとの間のマッピングを定義するために用いられる定義は、数学的定義、テーブル、ロードモジュール、またはその他の形態を取り得る。EVENTメソッドがアクセス要求を「ゼロ」個の原子エレメントにマップするときは、ユーザによ

りアクセスされたイベントは、特定の当てはまる原子エレメント定義に基づいたいかなる原子エレメントにもマップされない。これは、例えば、オブジェクトのオーナーが、そのようなアクセスに基づいて使用を計量することに興味がない場合（例えばオブジェクトのオーナーが計量の観点上そのようなアクセスは重要でないと見なすために）であり得る。

「ユーセージマップ」は、使用履歴情報を高い効率で格納するために、「ビットマップイメージ」を用いてもよい。ユーセージマップにおける個々の格納エレメントは、原子エレメントに対応し得る。一つのユーセージマップ中の異なるエレメントは、異なる原子エレメントに対応し得る（例えば、一つのマップエレメントは読まれたバイト数に対応し、別のマップエレメントは特定の章が開かれたか否かに対応し、更に別のマップエレメントが他の使用イベントに対応していてもよい。）

本発明の好適な実施態様で提供されるユーセージマップの特徴の一つは、マップエレメントの重要性が、少なくとも部分的には、ユーセージマップ中の位置によって特定されることである。このようにして、好適な実施態様で提供されるユーセージマップにおいて、マップエレメントによって示されたあるいは符号化された情報は、マップ構造中のその位置（物理的または論理的な）の関数である。一つの単純な例として、１２章からなる小説のためのユーセージマップは、小説の各章に対して１つのエレメントずつ、１２のエレメントからなっていてもよい。ユーザが第１章を開くとき、第１章に対応するエレメント中の一つ以上のビットが値を変更され得る（例えば「１」にセットされる）。この単純例において、小説を含むコンテンツオブジェクトのオーナーが、どの章がユーザによって開かれたかを計量することのみに興味がある場合は、ある章に対応するユーセージマップエレメントをユーザがその対応章を最初に開いたときに「１」にセットし、そのユーザがその章をさらに何回追加的に開こうが「１」のままに維持されることができる。オブジェクトのオーナーまたはその他の興味があるVDE参加者は、単にコンパクトなユーセージマップを調べてどのエレメントが「１」にセットされたかを決定することにより、どの章（単数または複数）がユーザにより開かれたかを素早く効率的に知ることができる。

ユーザが小説の各章を何回開いたかを、コンテンツオブジェクトのオーナーが知りたいとする。この場合、ユーセージマップは、１２章からなる小説の場合、各々がその小説の１２章のうちの異なる１つと１対１の対応を有するような、１２のエレメントを含み得る。ユーザが特定の章を開く各回毎に、対応するMETERメソッドが、対応するユーセージマップエレメントに含まれる値をインクリメントし得る。このようにして、アカウントを小説の各章に対して容易に維持することができる。

ユーセージマップ中のエレメントの位置は、多変数関数を符号化していてもよい。例えば、ユーセージマップ中のエレメントは、図２５Ｂに示すような２次元アレイに並べられてもよい。異なるアレイ座標は、例えば、原子エレメントおよび時間などの独立変数に対応してもよい。例として、コンテンツオブジェクトのオーナーが、音声録音のコレクションを含むオブジェクトを配布するとする。更に、コンテンツオブジェクトのオーナーは、ユーザがコレクション中の各録音を聴く回数を追い(track)、かつ月別に使用を追いたいとする。従って、コンテンツオブジェクトのオーナーは、１月の間にユーザが、各録音毎に、録音を何回聴いたかを知りたいと思っており、同様にこの同じ情報を２月、３月などに関して知りたいとする。この場合、ユーセージマップ（図２５Ｂ参照）は、エレメントの２次元アレイとして定義され得る。アレイの１つの次元は、音声録音ナンバーを符号化していてもよい。アレイの別の次元は、月を符号化していてもよい。１月の間、対応するMETERメソッドが、アレイ中の「１月」の列においてアレイ中のエレメントをインクリメントし、録音ナンバーの関数としてどのエレメントをインクリメントするかを選択する。１月が終わりに来れば、METERメソッドは１月の列のアレイエレメントへの書き込みをやめて、代わりに２月のための別のアレイエレメントのセットに値を書き込む－－この場合もやはりこの列中の特定のアレイエレメントを録音ナンバーの関数として選択する。このコンセプトは、Ｎ個の異なる変数を符号化するＮ次元にまで拡張することができる。

ユーセージマップ計量は、このように、以前の使用を参照するための効率的な手段である。ユーセージマップ計量は、連続性（相対的な連続性を含む）のテスト、論理的関連性（相対的な論理的関連性を含む）のテスト、使用のランダム化

および他の使用パターンなどの、ある種のVDE関連セキュリティ機能を可能にし得る。例えば、あるユーザによるコンテンツ使用の「ランダムさ」の程度や性質は、VDEコンテンツ予算制限を避けるための試みの、潜在的なインジケータとして機能し得る。ユーザまたはユーザのグループは、多数回のセッションを用いることによって、連続性、論理的関連性または量制限に違反はしないが、所与の価値あるコンテンツ単位の実質的な部分あるいは全部を再構築できるようなやり方で、コンテンツを抽出しようとするかも知れない。例えば、ある一定量の任意のあるいは特定のアトミックユニットの使用後の量ディスカウンティング、すなわちあるユーザが過去に無制限アクセス（またはある時間内における無制限アクセス）のために支払いを行った対象である情報コンテンツに再アクセスすることを可能にすることなどの、その他の有料使用パターン(pattern of usage for pricing)を決定するために、ユーセージマップを分析することができる。その他の有用な分析としては、所与のアトミックユニットについての複数回の使用に対するディスカウンティングがある。

マップ計量の更なる例としては、ユーザが使用するために支払いを行った（あるいは、使用したことが計量されたーー支払いまたは請求がまだであっても）全ての該当する原子エレメントの記録を格納することがある。そのようなユーセージマップは、同じ原子エレメントを後にユーザが使用することを可能にするための、非常に効率的かつ柔軟な手段をサポートできる。

更なるユーセージマップを、同じオブジェクトの不正使用(fraudlent usage)を検知するために維持することができる。例えば、オブジェクトは、長いブロックのシーケンシャルなアクセスが絶対に起こらないように格納され得る。そして、METERメソッドは、例えば、任意の指定された時間のインクリメントの間（例えば１０分、１時間、１日、１ヶ月、１年またはその他の期間）、全ての該当する原子エレメントアクセスを記録することができる。指定された時間インクリメントの終わりに、ユーセージマップを分析して、アクセスされたブロックのセットのうち異常に長い連続したものをチェックしたり、および／またはユーセージ

マップを該当する原子エレメントへの各アクセスの開始時に分析したりすることができる。もし各期間にもとづいた分析の後に何らの不正使用が検知されなければ、

ユーセージマップをクリア（あるいは部分的にクリア）しマッピングプロセス全体あるいはその一部を新しく開始することができる。もし不正使用が疑われるときあるいは検知されたときは、その情報を記録し、オブジェクトの使用を停止することができる。例えば、ユーザは、コンテンツプロバイダにコンタクトすることを要求されるかも知れない。するとコンテンツプロバイダは更に、使用情報を分析して更なるアクセスが許可されるべきか否かを決定する。

図２５ｃは、特定のタイプの「ワイドビットマップ」使用レコード1206を示す。ここで、使用レコードの各エントリは、特定の期間中の使用に対応する（例えば、今月の使用、先月の使用、先々月の使用など）。このように、図示の使用レコードは、「フラグ」のアレイまたはフィールド1206を含み、アレイ中の各エレメントは、この特定の例における異なる期間における使用を示すために用いられる。ある期間が終了すると、アレイ中の全てのエレメント1206を１ポジションずらすことによって、一連の複数期間における使用情報（またはユーザのアクセス権利の購入）を、一連の連続アレイエレメントに反映することができる。この図２５ｃに示す特定の例においては、ワイドアレイ1206全体が各月毎に１アレイポジションずらされ、最も古いアレイエレメントは削除され、新しいアレイエレメントが現期間に対応する新しいアレイマップに挿入("turned" in)される。この例において、レコード1302は、暦の今月ならびに今月の直前５ヶ月間中における、使用アクセス権利および／または使用関連行動を追っている。対応する課金および／または課金メソッド406はマップを検査し(inspect)、レコードに格納された使用データを用いる数式に基づいて、現使用についての課金および／またはセキュリティ監視に関連しての使用を決定し、ワイドレコードを、使用が起こったなどの該当アレイエレメントを示すように、更新する。ワイドビットマップは、エレメント単位の使用カウントの維持、または連続性、関連性などの上述の機能、または機能性の組み合わせなど、他の多くの目的に用い得る。

監査追跡マップは、制御、計量、予算、および課金メソッドならびに、これらメソッドに関連するロードモジュールによって決定される任意の頻度で、生成され得る。監査追跡は、計量および予算と同様な構造を有しており、監査追跡が生成される原因となった使用イベントに関する情報に加えて、ユーザ特異的な情報を含む。計量および予算と同様に、監査追跡は、コンテンツプロバイダまたはその承認された被指名人(designee)によって定義されるダイナミックなフォーマットを有し、上記テーブルに示した計量および予算と、基本エレメントタイプを共有している。これらのタイプに加えて、以下のテーブルに、監査追跡において見られる他の重要なデータフィールドの例を挙げる：

フィールドタイプ	フォーマット	典型的使用	使用の説明
使用イベントID	符号無し、長	計量／予算／課金	プロセスシーケンスを開始したイベントID。
内部シーケンスナンバー	符号無し、長	計量／予算／課金	不正改変された監査を検知するたすけとなる取引ナンバー。
原子エレメント（単数または複数）およびオブジェクトID	適切な幅を有する符号無しの整数（単数または複数）	計量／課金	使用されたオブジェクトのIDおよび原子エレメント（単数または複数）。
パーソナルユーザ情報	文字その他の情報	予算／課金	ユーザに関してのパーソナル情報。
使用日付／時刻	time_t	計量／予算／課金	使用日付／時刻。
サイトID／ユーザID	VDE ID	計量／予算／課金	ユーザのVDE ID。

ヘッダスペースを残すために、監査追跡レコードは、自動的に単一のレコードに結合されてもよい。結合プロセスは、例えば、個々の監査追跡レコードを作成

するロードモジュールの制御下で起こり得る。

パーミッションレコードの概観（Overview）

図１６はまた、PERC808が安全データベース610の一部として格納され得ることを示している。パーミッションレコード（PERC）808は、VDE100の好適な実施態様によって提供されるデータ駆動制御階層の最高レベルに位置する。基本的に、VDE100によって配布される各情報および／または取引コンテンツに対応して、少なくとも一つのPERC808が存在する。従って、好適な実施態様において、各VDEオブジェクト300に対して少なくとも一つのPERC808が存在する。複数の対応PERC808を有するオブジェクトもある。PERC808は、アクセスおよび／または操作パーミッションがどのように配布されるか、および／またはコンテンツおよび／またはその他の情報が他にどのように使用されるかを制御する。PERC808はまた、コンテンツおよび／またはその他の情報における、あるいはこれらに対するVDE参加者の「権利」を指定する。

好適な実施態様において、いかなるエンドユーザも、パーミッションレコード808がそのエンドユーザに配送（deliver）されなければ、VDEオブジェクトを使用またはアクセスしてはならない。上述したように、PERC808は、移動（traveling）オブジェクト860の一部として配送されるか、あるいは別途配送される（例えば管理オブジェクトの中で）。電子機器600は、対応するPERC808が存在しなければオブジェクトにアクセスしてはならず、PERCに含まれる制御構造によって許可されたオブジェクトおよび関連情報のみを使用できる。

端的に言えば、PERC808は、対応するVDEオブジェクト300に関するメソッド、メソッドオプション、復号化鍵および権利についての情報を格納する。

PERC808は、高レベルの動作カテゴリーあるいは分類を定義する、制御構造を含んでいる。これらの高レベルカテゴリーは、「権利」と呼ばれる。「権利」制御構造は、それ自体、「メソッド」1000を参照する内部制御構造を提供する。好適な実施態様のPERC808における内部構造は、オブジェクトまたは関連制御構造（PERC自体に対して行われる動作を含む）に対して許される各動作を行うために必要な「メソッド」を組織（organize）する。例えば、PERC808は、オブジェクト

に対する復号化鍵を含んでおり、鍵の使用は、PERCが「権利」の行使に関連する動作を行うために必要とするメソッドによって、制御される。

あるオブジェクトに対するPERC808は典型的には、オブジェクトが作成されるときに作成され、PERCの将来における実質的な改変物は、許されれば、動作に関連するメソッドにより、同じ（または異なる）PERCによって定義される配布権利（単数または複数）を用いて、制御される。

図２２は、好適な実施態様の提供するPERC808の一例において存在する、内部構造を示す。図示した構造の全ては、対応オブジェクトを特定の方法で処理するために必要なメソッドの集合(collection)を表す（または参照する）。PERC808は階層構造として組織され、その階層の基本エレメントは以下の通りである：

「権利」レコード906

「制御セット」914

「必須(required)メソッド」レコード920　および

「必須メソッドオプション」924。

PERC808階層に含められ得るエレメントで、規則セットのネゴシエーションをサポートするための規則および規則オプション、ならびにスマートオブジェクトおよびユーザのパーソナル情報をプライバシーフィルタによって保護するための制御情報を記述する、他のエレメントもある。これらの別エレメントは以下を含み得る：

オプション権利レコード

オプション制御セット

オプションメソッドレコード

パーミッションを与えられた権利レコード

パーミッションを与えられた権利制御セット

パーミッションを与えられたメソッドレコード

必須DTD記述

オプションDTD記述

パーミッションを与えられたDTD記述

これら別フィールドは、これらフィールドのコンテンツに対するその動作に関するネゴシエーションまたは決定の基盤に部分的になる他のプロセスを、制御し得る。権利ネゴシエーション、スマートオブジェクト制御情報、および関連プロセスは、その動作のより正確な制御のために、これらのフィールドを用い得る。

図２６に示すPERC808は、PERCヘッダ900、CS0（「制御セット０」）902、秘密本体鍵(private body key)904、および一つ以上の権利サブレコード906を含む。好適な実施態様における制御セット０902は、オブジェクト300に関連する一つ以上の「権利」に共通の情報を含んでいる。例えば、ある特定の「イベント」メソッドまたは複数のメソッドは、使用権利、抽出権利および／またはその他の権利について同一であるかも知れない。この場合、「制御セット０」902は、複数の「権利」にわたって共通なこのイベントを参照し得る。実際には、PERC808の複数の「権利」レコード906の各々内に共通に用いられるイベントの異なるインスタンスを格納することが可能であるので、「制御セット０」902の提供は最適化ということになる。

各権利レコード906は、１つのオブジェクトに対応する異なる１つの「権利」を定義する。「権利」レコード906は、PERC808に存在する組織の最高レベルである。PERC808中にはいくつかの異なる権利が存在し得る。「権利」とは、VDE100の基本アーキテクチャの参加者によって望まれる主要な機能的区分(functional partition)を表す。例えば、オブジェクトを使用する権利と、オブジェクトを使用する権利を配布する権利とは、VDE100内における主要な機能グループをなす。可能性のある権利の例としては、コンテンツへのアクセス、コンテンツへアクセスするパーミッションを配布する権利、コンテンツおよび／または制御構造に関連する監査追跡を読みかつ処理する能力、コンテンツおよび／または関連する制御構造（銀行取引、カタログ購入、税徴収、EDI取引など）に関連する取引または関連しない取引を行う権利、ならびに他のユーザへの配布のために作成されたPERCの内部構造の全部または一部を変更する能力がある。PERC808は、PERCが賦与(grant)するオブジェクトアクセス／使用権利の各タイプについて、権利レコード906を含む。

通常、VDEのエンドユーザにとって、最も頻繁に賦与される権利は使用権である。他のタイプの権利としては「抽出権」、エンドユーザの監査追跡情報にアクセスするための「監査権」、およびオブジェクトを配布するための「配布権」がある。これら各々のタイプの権利は、異なる権利レコード906の形で実現し得る

（または１つのオブジェクトに対応する異なるPERC808を異なる権利を賦与するために用いてもよい）。

各権利レコード906は、権利レコードヘッダ908、CSR（「権利のための制御セット」）910、一つ以上の「権利鍵」912、および一つ以上の「制御セット」914を有している。各「権利」レコード906は、その「権利」の行使においてオブジェクトを制御するための必須のあるいは選択可能なオプションである、一つ以上の制御セット914を有している。従って、次のレベルにおいて、「権利」906の内側に、制御セット914がある。各制御セット914は、それ自体、制御セットヘッダ916、制御メソッド918、および一つ以上の必須メソッドレコード920を有する。各必須メソッドレコード920は、それ自体、必須メソッドヘッダ922および一つ以上の必須メソッドオプション924を有する。

VDE100において、２つのタイプの制御セット914が存在する：「制御セット０」または「権利のための制御セット」というデジグネータを与えられる共通必須制御セットと、制御セットオプションのセットとである。「制御セット０」902は、全ての制御セットオプションに共通の必須メソッドのリストを含んでおり、共通に必須であるメソッドが各制御セットオプション内で複製されなくてもよいようになっている。「権利のための制御セット（「CSR」）」910は、所与の権利内において、制御セットの同様なリストを含んでいる。「制御セット０」および任意の「権利のための制御セット」は従って、上述のように、最適化と言うことになる。各制御セットオプションにおける全ての共通の必須メソッドをリストしかつ「制御セット０」および任意の「権利のための制御セット」を省略することによっても、制御セットの関して同じ機能性が達成できる。

制御セットオプションの一つ、「制御セット０」、および適切な「権利のための制御セット」は、権利を行使するために必要な完全な制御セットを、全体とし

て形成する。

各制御セットオプションは、必須メソッド1000のリストを含み、権利が行使され得る異なる方法を表している。好適な実施態様において権利を行使する任意の１回につき、可能な完全制御セット914のうち１つのみが用いられる。

各制御セット914は、作成者および／または配布者が権利を行使するための全ての要件を満足するために必要なだけの数の、必須メソッドレコード920を含む。権利を行使し得る複数の方法または、所与の権利が行使される方法を支配する複数の制御セットの両方が、サポートされる。例として、単一の制御セット914が、オブジェクトのコンテンツを読むために多数の計量および予算メソッドを必要とし、またオブジェクトのコンテンツを印刷するために異なる計量および予算を必要とするかも知れない。オブジェクトのコンテンツを読むことおよび印刷することの両方が、単一の制御セット914において制御され得る。

または、２つの異なる制御セットオプションによっても、一方の制御セットオプションを用いて読まれたバイト数の計量および予算決めをサポートし、他方の制御セットオプションを用いて読まれた段落の数の計量および予算決めをサポートすることによって、オブジェクトのコンテンツを読むことをサポートできる。ある１つの時点においてこれらのオプションの一方または他方がアクティブとなる。

典型的には、各制御セット914は関連メソッドの１セットを参照し、従って異なる制御セットはメソッドオプションの異なるセットを提供し得る。例えば、ある制御セット914は１つの種類の固有の(distinct)計量方法論を表し、別の制御セットが別の全く異なる固有の計量方法論を表してもよい。

次のレベルにおいて、制御セット914の内側に、必須メソッドレコード920がある。好適な実施態様において、メソッドレコード920は、メソッド1000を含むか、あるいは参照する。メソッド1000は、「イベント」の集合、これらのイベントと関連するロードモジュールへのリファレンス、スタティックデータ、および、イベントを処理するために必要であり得る他の任意の別途デリバラブルなデータエレメント（例えばUDE）の自動的な検索(retrieval)のための、安全データベー

ス６１０へのリファレンスである。制御セット９１４は、特定の権利（すなわち権利に関連する処理イベント）を行使するために用いられなければならない必須メソッドのリストを含む。制御セット９１４中にリストされた必須メソッドレコード９２０は、制御セットがサポートする、権利を行使するためのメソッドが存在しなければならないことを示す。必須メソッドは、後述の「ロードモジュール」１１００を参照し得る。簡単に言えば、ロードモジュール１１００は、必須メソッドを実行するために

用い得る実行可能コードの断片である。

各制御セット９１４は、その必須メソッドの１つとして、制御メソッドレコード９１８を有し得る。参照された制御メソッドは、制御セット９０６によって定義される様々なメソッド１０００の一部または全部の間の関係を、定義し得る。例えば、制御メソッドは、どの必須メソッドが、特定のイベントを処理するための機能的に同一なグループに入れられるか、および必須メソッドを処理するための順序を示し得る。従って、制御メソッドは、レコード９２０(a)(1)(i)によって参照される必須メソッドが最初にコールされるものであり、そしてその出力はレコード９２０(a)(1)(ii)によって参照必須メソッドに行く、などのことを指定し得る。このようにして、計量メソッドは、１つ以上の課金メソッドに結びつけられ得、課金メソッドは異なる予算メソッドなどに個々に結びつけられ得る。

必須メソッドレコード９２０は、一つ以上の必須メソッドオプション９２４を指定する。必須オプションは、好適な実施態様におけるPERC８０８における制御構造の最低レベルである。必須メソッドをパラメータ化し、必須メソッドオプション９２４を必須メソッドとは独立に指定することにより、必須メソッドを多くの異なる状況において再使用することが可能になる。

例えば、必須メソッドレコード９２０は、その必須メソッドについての必須メソッドオプションリストの予算メソッドIDのリストから、実際の予算メソッドIDが選ばれなければならないことを示し得る。この場合の必須メソッドレコード９２０は、必須とされるメソッドのタイプに関する情報については、メソッドIDを含まず、あるメソッドが必須とされていることを示すだけである。必須メソッドオプ

ション924は、この必須メソッドオプションが選択された場合、使用されるメソッドの、メソッドIDを含む。更なる最適化として、もし特定の必須メソッドに対してオプションが一つしか存在しないならば、実際のメソッドIDを格納してもよい。これにより、このデータ構造のサイズが減少する。

PERC808はまた、オブジェクト300のための基本復号化鍵およびその他の任意の「権利」（例えば監査追跡を符号化および／または非符号化(decoding)するための）とともに使用される鍵を含んでいる。オブジェクトコンテンツの鍵または、オブジェクトのコンテンツを復号化するために用い得る他の鍵を含むようなオブジェクトの一部を復号化するための鍵を、含んでいてもよい。鍵の使用は、PERC808内の同じ「権利」906中の制御セット914によって制御される。

より詳細には、図２６に示すPERC808は秘密本体鍵904、および権利鍵912を含んでいる。秘密本体鍵904は、対応するVDEオブジェクト300の秘密本体鍵806中に含まれる情報を復号化するために用いられる。このような情報は例えば、メソッド1000、ロードモジュール1100および／またはUDE1200を含む。権利鍵912は、好適な実施態様において権利を行使するために用いられる鍵である。そのような鍵912は例えば、PERC808によって指定されたメソッドがコンテンツを復号化してVDEノードによってエンドユーザに放出することを可能にするための、暗号化鍵を含む。これらの権利鍵912は、好適な実施態様において、オブジェクト300に対してユニークである。好適な実施態様において、その使用は好ましくは予算によって制御される。

PERC808の詳細例

図２６Ａおよび２６Ｂは、好適な実施態様のPERC808の一例を示す。本例において、PERCヘッダ900は、以下を有する：

サイトレコードナンバー926、

秘密本体鍵ブロックの長さを指定するフィールド928、

PERCの長さを指定するフィールド930、

PERCの失効日および／または時刻を指定する失効日／時刻フィールド932、

PERC808が改変された最後の日および／または時刻を指定する最終改変日／時刻フィールド934、

誰が元々PERCおよび／または対応オブジェクトを配布したかを指定する、オリジナル配布者IDフィールド936、

誰がPERCおよびまたはオブジェクトの最終配布者だったかを指定する最終配布者フィールド938、

対応するVDEオブジェクト300を識別するオブジェクトIDフィールド940、

詳細（particulars）において異なり得る同じタイプのPERCをレコードクラスが区別するための、PERCおよび／またはインスタンスIDのクラスおよび／またはタイプを指定するフィールド942、

PERC内の「権利」サブレコード906の数を指定するフィールド944、および

有効性検査タグ948。

図２６ａ、図２６ｂに示すPERC808はまた、秘密本体鍵ブロック950に格納される秘密本体鍵を有する。

このPERC808は、PERC内の全ての権利906によつて共通に使用される制御セット０サブレコード914(0)を有する。この制御セット０レコード914(0)は、以下のフィールドを有し得る：

制御セット０レコードの長さを指定する長さフィールド952

制御セット内の必須メソッドレコード920の数を指定するフィールド954

レコードの改変を制御するためのアクセスタグを指定するアクセスタグフィールド956および

一つ以上の必須メソッドレコード920。

各必須メソッドレコード920は、それ自体、以下を有し得る：

必須メソッドレコードの長さを指定する長さフィールド958

必須メソッドレコード920のメソッドオプションレコード数を指定するフィールド960

レコードの改変を制御するためのアクセスタグを指定するアクセスタグフィールド962および

一つ以上の必須メソッドオプションレコード924。

各メソッドオプションサブレコード924は、以下を有し得る：

メソッドオプションレコードの長さを指定する長さフィールド964

メソッドオプションレコードに対応するデータ領域（あれば）の長さを指定する長さフィールド966

メソッドID（例えばタイプ／オーナー／クラス／インスタンス）を指定するメソッドIDフィールド968

フィールド968で指定されたメソッドと関連付けるためのコリレーションタグを指定するコリレーションタグフィールド970

このレコードの改変を制御するためのアクセスタグを指定するためのアクセスタグフィールド972

メソッド特異的属性フィールド974

データ領域976および

有効性検査用のチェック値フィールド978

本例のPERC808はまた、一つ以上の権利レコード906および全体(overall)チェック値フィールド980を有する。図２３ｂは、図１６ａに示す権利レコード906の一つの例である。この特定の例において、権利レコード906ａは、以下を有する権利レコードヘッダ908を有する：

権利鍵ブロック912の長さを指定する長さフィールド982

権利レコード908の長さを指定する長さフィールド984

権利レコードの失効日および／または時刻を指定する失効日／時刻フィールド986

権利を識別する権利IDフィールド988

権利レコード906内の制御セット914の数を指定する数フィールド990、および

権利レコードの改変を制御するためのアクセスタグを指定するアクセスタグフィールド992。

本例の権利レコード906は、以下を有する：

この権利のための制御セット(CSR)910

権利鍵ブロック912

一つ以上の制御セット914、および

チェック値フィールド994。

オブジェクトリジストリ(object registry)

図１６を再び参照して、安全データベース610は、「登録された」オブジェクトのための「ルックアップ」メカニズムをサポートする、データ構造を提供する。

この「ルックアップ」メカニズムは、電子機器600が、VDEオブジェクト300を、安全な方法でPERC808、メソッド1000およびロードモジュール1100と対応付ける(associate)ことを可能にする。好適な実施態様において、このルックアップメカニズムは、オブジェクトリジストリ450内部に含まれるデータ構造に一部基づいている。

一実施態様において、オブジェクトリジストリ450は、以下のテーブルを有する：

・オブジェクト登録テーブル460；

・サブジェクト(subject)テーブル462；

・ユーザ権利テーブル（「URT」）464；

・管理的イベントログ442；

・発送(shipping)テーブル444；および

・受信(receiving)テーブル446。

本実施態様例におけるオブジェクトリジストリ460は、登録されたVDEオブジェクト300およびこれらオブジェクトに関するユーザおよびユーザグループの権利に関する情報のデータベースである。電子機器600が新しい予算またはロードモジュール1100を含むオブジェクト300を受信するとき、電子機器は通常、オブジェクトに含まれる情報を安全データベース610に追加する必要がある。また、任意の新しいVDEオブジェクト300が電子機器600に到着したとき、電子機器は、オ

ブジェクトをオブジェクトリジストリ450に「登録」することによってアクセス可能にしなければならない。新しいオブジェクト300のためのリストおよびレコードは、好適な実施態様において、オブジェクトが電子機器600によって「登録される」ときに構築される。オブジェクトについての情報は、オブジェクトの暗号化された秘密ヘッダ、オブジェクト本体、暗号化された名前サービスレコードから得られ得る。この情報は、SPE503によってオブジェクト300から導かれても、抽出されてもよく、その後安全データベース610中に暗号化レコードとして格納され得る。

一実施態様において、オブジェクト登録テーブル460は、情報識別オブジェクトを、オブジェクト格納部(storage)(格納場所(repository))728内に有する。

オブジェクト格納部728内に格納されたこれらのVDEオブジェクト300は、この実施態様例において、安全データベース610の必要部分ではない。なぜなら、オブジェクトは典型的には自分自身のセキュリティ（必要に応じて）を導入しており、安全データベースを維持するために用いられるものとは異なるメカニズムを用いて維持されるからである。VDEオブジェクト300は厳密には安全データベース610の一部ではないかも知れないが、オブジェクトリジストリ450（および特にオブジェクト登録テーブル460）は、オブジェクトを参照(refer to)するため、結果としてオブジェクトを安全データベース610内に「援用」することになる。好適な実施態様において、電子機器600は、対応登録レコードをオブジェクト登録テーブル460内に格納して適切に登録されていないオブジェクト300を使用することを、不可能にされる(disabled)ことができる。

本実施態様例におけるサブジェクトテーブル462は、オブジェクト登録テーブル460によって参照されるオブジェクトと電子機器600のユーザ（またはユーザグループ）との間に、対応関係を確立する。サブジェクトテーブル462は、以下に説明するように、アクセス制御リスト（「ACL」）の属性の多くを提供する。

実施態様例におけるユーザ権利テーブル464は、パーミッションその他の特定のユーザまたはユーザグループに特異的な情報および、サブジェクトテーブル462中に述べられるオブジェクトの組み合わせを提供する。実施態様例において、

パーミッションレコード808（図１６にも示され、安全データベース610内に格納されている）は、特定のオブジェクト－ユーザ組み合わせにおけるパーミッションの全体(universe)を提供し得る。ユーザ権利テーブル464内のレコードは、例えばオブジェクト登録時におけるインタラクション中にユーザによってなされた選択に基づいて、このパーミッション全体のサブセットを指定し得る。

管理的イベントログ442、発送テーブル444、および受信テーブル446は、VDEオブジェクト300の受け取りと配送に関する情報を提供する。これらのデータ構造は、電子機器600によって送り受けされる管理的オブジェクトを追い、例えば、管理的オブジェクトの目的および動作を簡略化形式および詳細形式にしたものを含む。端的には、発送テーブル444は、電子機器600によって別のオブジェクト参加者に送られた（または送ることが予定(schedule)されている）各管理的オブジェクトに対する発送レコードを含む。好適な実施態様における受信テーブル446は、電子機器600によって受信された（または受信されることが予定されている）各管理的オブジェクトに対する受信レコードを含む。管理的イベントログ442は、各発送された管理的オブジェクトおよび各受信された管理的オブジェクトに対するイベントログレコードを含み、受信された管理的オブジェクトによって指定された各別のイベントに関する詳細を含み得る。

管理的オブジェクト発送および受信

図２７は、発送テーブル444のための詳細なフォーマットの一例を示す。好適な実施態様において、発送テーブル444は、ヘッダ444Aおよび任意の数の発送レコード445を含む。ヘッダ444Aは、発送テーブル444を維持するために使用される情報を有している。発送テーブル444内の各発送レコード445は、発送イベントに関する詳細を提供する（すなわち、別のVDE参加者への管理的オブジェクトの完了した発送であるか、管理的オブジェクトの予定された発送であるか）。

本実施態様例の安全データベース610においては、発送テーブルヘッダ444Aは、サイトレコードナンバー444A(1)、ユーザ（またはグループ）ID 444A(2)、一連のリファレンスフィールド444A(3)～444A(6)、有効性検査タグ444A(7)～444A(8)、およびチェック値フィールド444A(9)を含み得る。一連のリファレンスフィ

ールド444A(3)～444A(6)は、発送テーブル444内の発送レコード445のリストをデジグネートする特定の最近のIDを、参照する。例えば、フィールド444A(3)は、管理的オブジェクトの完了した出発側の発送(outgoing shipping)を表す「最初の」発送レコードを参照し、フィールド444A(4)は、管理的オブジェクトの完了した出発側の発送を表す「最後の」発送レコードを参照し得る。この例において、「最初」および「最後」は、所望であれば、一つの例として、発送の時刻または順序を指していてもよい。同様に、フィールド445A(5)および444A(6)は、予定された出発側の発送の「最初」および「最後」の発送レコードを参照してもよい。有効性検査タグ444A(7)は、ヘッダ中のユーザ（グループ）IDに対応する名前サービスレコードテーブル452内の名前サービスレコードから、有効性検査を提供し得る。このことにより、発送レコードから、発送レコードに記述されたオブジ

エクトの送り手を記述する名前サービスレコードへと戻るアクセスが、可能になる。有効性検査タグ444A(8)は、一つ以上のポインタ444A(3)～444A(6)によって参照される「最初の」出発側発送レコードに対し、有効性検査を提供する。予定された発送レコードの有効性検査のために、他の有効性検査タグを提供してもよい。

図示の発送レコード444(1)は、サイトレコードナンバ-445(1)(A)を含む。また、最初および最後の予定された発送日／時刻445(1)(B)、445(1)(C)も含んでおり、管理的オブジェクト発送のスケジューリングに使用される時刻のウィンドウを提供する。フィールド445(1)(D)は、管理的オブジェクトの完了した発送の実際の日付／時刻を指定する。フィールド445(1)(E)は、発送されたまたは発送されるべき管理的オブジェクトのIDを提供することによって、オブジェクト格納部728内のどの管理的オブジェクトがこの特定の発送レコードに属するかを識別する。リファレンスフィールド445(1)(G)は、名前サービスレコードテーブル452内の、発送されたまたは発送されるべき管理的オブジェクトの実際のまたは意図された受信者(recipient)を指定する、名前サービスレコードを参照する。名前サービスレコードテーブル452内のこの情報は、例えば、図１２に示す出発側の管理

的オブジェクトマネージャ754が、管理的オブジェクトを意図された受信者に発送するようにオブジェクトスイッチ734に告知(inform)することを可能にするのに十分なルーティング情報を提供してもよい。フィールド445(I)(H)は、管理的オブジェクトの発送の目的を指定し得（例えば一連のビットフラグを用いて）、フィールド445(I)(I)は発送のステータスを指定し得る。リファレンスフィールド445(I)(J)、445(I)(K)は、リンクされたリスト中の「前回」および「次回」発送レコード445を参照し得る（好適な実施態様において、一方が完了した発送レコード用、他方が予定された発送レコード用の、２つのリンクされたリストがあってもよい）。フィールド445(I)(L)～445(I)(P)は各々、ヘッダ444Aからの有効性検査タグ、ポインタ445(I)(F)によって指し示された管理的イベントログ442中のレコードへの有効性検査タグ、フィールド445(I)(G)によって参照された名前サービスレコードへの有効性検査タグ、445(I)(J)によって参照された前レコードからの有効性検査タグ、およびフィールド445(I)(K)によって参照される次レコードへの有効性検査タグを、提供してもよい。発送レコード445の有効性検査のためにチェック値フィールド445(I)(Q)を用いてもよい。

図２８は、受信テーブル446の詳細なフォーマットの一つの可能性の例を示している。一実施例において、受信テーブル446は、図２７に示す発送テーブル444の構造と同様な構造を有する。従って、例えば、受信テーブル446はヘッダ446aおよび、各々が管理的オブジェクトの特定の受信または予定された受信に関する詳細を含む、複数の受信レコード447を有し得る。受信テーブル446は、一方が完了した受信用、他方が予定された受信用の、２つのリンクされたリストを含んでもよい。受信テーブルレコード447は各々、名前サービスレコードテーブル452内の、管理的オブジェクトの送り手を指定するエントリを参照し、管理的イベントログ442内のエントリを各々指し示してもよい。受信レコード447はまた、予定されたおよび／または完了した受信に関しての追加的な詳細（例えば予定されたまたは実際の受信日付／時刻、受信の目的および、受信のステータス）を含んでいてもよく、また各々、他の安全データベースのレコードへの参照を有効性検査するための有効性検査タグを含んでいてもよい。

図２９は、管理的イベントログ442の詳細なフォーマットの一例を示す。好適な実施態様において、管理的イベントログ442は、各発送された管理的オブジェクトおよび各受信された管理的オブジェクトに対する、イベントログレコード442(1)...442(N)を有する。各管理的イベントログレコードは、ヘッダ443aおよび、１～Ｎのサブレコード442(J)(1)...442(J)(N)を有していてもよい。好適な実施態様において、ヘッダ443aはサイトレコードナンバーフィールド443A(1)、レコード長フィールド443A(2)、管理的オブジェクトIDフィールド443A(3)、イベント数を指定するフィールド443A(4)、発送テーブル444または受信テーブル446からの有効性検査タグ443A(5)、およびチェックサムフィールド443A(6)を有していてもよい。フィールド443A(4)で指定されたイベント数は、管理的イベントログレコード442(J)内のサブレコード442(J)(1)...442(J)(N)の数に対応する。これらサブレコードの各々は、フィールド443(A)(3)内に指定された管理的オブジェクトに影響されるあるいは対応する、特定の「イベント」に関する情報を指定する。管理的イベントは、管理的イベントログ442内に保持されることにより、システ

ムから送られたあるいは受信された管理的オブジェクトの再構築（および構築または処理のための準備）を可能にする。これにより、失われた管理的オブジェクトを、後に再構築することが可能になる。

各サブレコードは、サブレコード長フィールド442(J)(1)(a)、データ領域長フィールド442(J)(1)(b)、イベントIDフィールド442(J)(1)(c)、レコードタイプフィールド442(J)(1)(d)、レコードIDフィールド442(J)(1)(e)、データ領域フィールド442(J)(1)(f)、およびチェック値フィールド442(J)(1)(g)を有していてもよい。データ領域442(J)(1)(f)は、イベントIDフィールド442(J)(1)(c)で指定されたイベントによって安全データベース610内のどの情報が影響されるか、またはどのような新しい安全データベースアイテムが追加されたかを示すために用いられ得、また、イベントの結果を明示(specify)してもよい。

好適な実施態様におけるオブジェクト登録テーブル460は、オブジェクト格納部（格納場所）728内の各VDEオブジェクト300に対応するレコードを、含む。新

しいオブジェクトが到着したか、あるいは検知されたとき（例えばリダイレクタ(redirector)684によって）、好適な実施態様における電子機器600は、適切なオブジェクト登録レコードを作成してオブジェクト登録テーブル460に格納することにより、オブジェクトを「登録」する。好適な実施態様において、オブジェクト登録テーブルは、ユーザ非依存であって所与のVDE電子機器600に登録されたオブジェクトのみに依存する情報を、格納する。登録動作は典型的には、オブジェクトに関連するREGISTERメソッドによって管理される。

本例において、サブジェクトテーブル462は、ユーザ（またはユーザのグループ）を、登録されたオブジェクトと対応付ける。例におけるサブジェクトテーブル462は、どのユーザがどの登録されたVDEオブジェクト300にアクセスすることを承認されているかを指定することによって、アクセス制御リストの機能を果たす。

上述のように、安全データベース610は、各登録されたVDEオブジェクト300に対応する少なくとも一つのPERC808を、格納する。PERC808は、対応するVDEオブジェクト300を使用またはこれにアクセスするために行使され得る、権利のセットを指定する。好適な実施態様においては、ユーザは、対応するPERC808によって承認された権利のサブセットを選択することおよび／またはPERC808によって付与される権利の一部または全部に対応するパラメータまたは選択を指定することによって、そのアクセス権利を「カスタマイズ」することが可能にされる。これらのユーザによる選択は、好適な実施態様において、ユーザ権利テーブル464中において述べられる。ユーザ権利テーブル（URT）464は、各々が一人のユーザ（またはユーザグループ）に対応する、URTレコードを有する。これらのURTレコードの各々は、対応するVDEオブジェクト300についての、ユーザ選択を指定する。これらのユーザ選択は、独立にまたはPERC808と協力して、URTレコード内に含まれる選択によって指定される方法で、PERC808によってユーザに付与された権利を行使するために、一つ以上のメソッド1000を参照し得る。

図３０は、これらの様々なテーブルが、互いに相互作用して安全データベースルックアップメカニズムを提供する様子を示す、一例である。図３０に図示する

オブジェクト登録テーブル460は、複数のオブジェクト登録レコード460(1)、460(2)、...を有する。これらのレコードは、オブジェクト格納場所728内に格納されたVDEオブジェクト300(1)、300(2)...に対応する。図３１は、好適な実施態によって提供されるオブジェクト登録レコード460のフォーマットの一例を示す。オブジェクト登録レコード460(N)は、以下のフィールドを含み得る：

サイトレコードナンバーフィールド466(1)

オブジェクトタイプフィールド466(2)

作成者IDフィールド466(3)

オブジェクトIDフィールド466(4)

サブジェクトテーブル462を参照するリファレンスフィールド466(5)

属性フィールド466(6)

最小登録インタバルフィールド466(7)

サブジェクトテーブルレコードへのタグ466(8)、および

チェック値フィールド466(9)。

サイトレコードナンバーフィールド466(1)は、このオブジェクト登録レコード460(N)に対するサイトレコードナンバーを指定する。安全データベース610の一

実施態様において、安全データベース内に格納された各レコードは、サイトレコードナンバーによって識別される。このサイトレコードナンバーは、安全データベース610内の全てのレコードを追うために、データベースルックアッププロセスの一部として、用い得る。

オブジェクトタイプフィールド466(2)は、VDEオブジェクト300のタイプを指定し得る（例えばコンテンツオブジェクト、管理的オブジェクトなど）。

本例における作成者IDフィールド466(3)は、対応するVDEオブジェクト300の作成者を識別し得る。

本例におけるオブジェクトIDフィールド466(4)は、登録されたVDEオブジェクト300をユニークに識別する。

好適な実施態様におけるリファレンスフィールド466(5)は、サブジェクトテーブル462中のレコードを識別する。このリファレンスの使用により、電子機器600

は、サブジェクトテーブル462にリストされている、対応するVDEオブジェクト300にアクセスすることを承認された全てのユーザ（またはユーザグループ）を決定し得る。タグ466(8)は、フィールド466(5)を用いてアクセスされたサブジェクトテーブルレコードが、オブジェクト登録レコード460(N)とともに用いられる適切なレコードであることの有効性検査のために、用い得る。

属性フィールド466(6)は、VDEオブジェクト300に対応する一つ以上の属性または属性フラグを、格納し得る。

最小登録インタバルフィールド466(7)は、エンドユーザがVDEオブジェクト300のユーザとして、情報交換所サービス、VDE管理者、またはVDEプロバイダに何回再登録し得るかを指定し得る。頻繁な再登録を防ぐことの一つの理由は、ユーザが、移動オブジェクト(traveling object)において予算量を再使用することを、指定された時間が経過するまで禁止する(foreclose)ことである。オブジェクトのオーナーが再登録を制限したくないときは、最小登録インタバルフィールド466(7)は、未使用にしておいてもよい。

チェック値フィールド466(9)は、レコードの安全性および完全性を確実にするためにレコード460(N)の不正化(corruption)または改変を検知するために使用される、有効性検査情報を含んでいる。好適な実施態様において、（安全データベース610内の他のレコードと同様に）レコード460(N)内の多くのまたは全てのフィールドは、全体的にあるいは部分的に暗号化されているか、および／または各レコードに冗長に格納されたフィールドを含んでいる（非暗号化形態で一度、および暗号化形態でもう一度）。同じフィールドの暗号化バージョンおよび非暗号化バージョンは、レコードの不正または改変を検知するために、様々な時点においてクロスチェックされる。

上述のように、リファレンスフィールド466(5)は、サブジェクトテーブル462を参照し、特に、サブジェクトテーブル内の一つ以上のユーザ／オブジェクトレコード460(M)を参照する。図３２は、本例で提供されるユーザ／オブジェクトレコード462(M)のためのフォーマットの一例を示す。レコード462(M)は、ヘッダ468およびサブジェクトレコード部470を有し得る。ヘッダ468は、サブジェクト登

録テーブル462内に含まれる「最初の」サブジェクトレコード470を参照するフィールド468(6)を含み得る。「最初の」サブジェクトレコード470(1)は、それ自身、サブジェクト登録テーブル462内の「次の」サブジェクトレコード470(2)を参照するリファレンスフィールド470(5)を含み得る、と続いていく。この「リンク化リスト」構造により、単一のオブジェクト登録レコード460(N)が１～Ｎのサブジェクトレコード470を参照することが可能になる。

本例におけるサブジェクト登録テーブルヘッダ468は、ヘッダを安全データベース610内のレコードとしてユニークに識別し得る、サイトレコードナンバーフィールド468(1)を有している。ヘッダ468はまた、オブジェクト登録テーブル作成者IDフィールド466(3)のコンテンツのコピーであってもよい、作成者IDフィールド468(2)を有し得る。同様に、サブジェクト登録テーブルヘッダ468は、オブジェクト登録テーブル460内のオブジェクトIDフィールド466(4)のコピーであってもよい、オブジェクトIDフィールド468(5)を有し得る。これらのフィールド468(2)、468(5)は、ユーザ／オブジェクト登録レコードを、明示的に(explicitly)特定のVDEオブジェクト300に対応させる。

ヘッダ468はまた、有効性検査を可能にするタグ468(7)を有し得る。一構成例において、ユーザ／オブジェクト登録ヘッダ468内のタグ468(7)は、このユーザ／オブジェクト登録ヘッダを指し示すオブジェクト登録レコード460(N)内のタグ466(8)と同じであってもよい。これらタグ468(7)および466(8)間の対応により、オブジェクト登録レコードおよびユーザ／オブジェクト登録ヘッダがマッチすることの、有効性検査が可能になる。

ユーザ／オブジェクトヘッダ468はまた、対応VDEオブジェクト300の元々の配布者を示すオリジナル配布者IDフィールド468(3)と、オブジェクトの処理チェーン中において、電子機器600に受け取られる以前の最終配布者を示す最終配布者IDフィールド468(4)とを、含んでいる。

ヘッダ468はまた、ヘッダと、フィールド468(6)が参照する「最初の」サブジェクトレコード470(1)との間の有効性検査を可能にする、タグ468(8)を含んでいる。

サブジェクトレコード470(1)は、サイトレコードナンバー472(1)、ユーザ（またはユーザグループ）IDフィールド472(2)、ユーザ（またはユーザグループ）属性フィールド472(3)、ユーザ権利テーブル464を参照するフィールド472(4)、（存在すれば）「次の」サブジェクトレコード470(2)を参照するフィールド472(5)、ヘッダタグ468(8)によって有効性検査を行うために使用されるタグ472(6)、フィールド472(4)によって参照されるユーザ権利テーブルレコード中の対応タグによって有効性検査を行うために使用されるタグ472(7)、フィールド472(5)によって参照される「次の」サブジェクトレコードタグによって有効性検査を行うために使用されるタグ472(9)、およびチェック値フィールド472(9)を有している。

ユーザまたはユーザグループID472(2)は、フィールド468(5)中で識別されるオブジェクトを使用することを承認されたユーザまたはユーザグループを、識別する。このように、フィールド468(5)および472(2)は共に、サブジェクトテーブル462によって提供されるアクセス制御リストの中核を形成する。ユーザ属性フィールド472(3)は、フィールド472(2)に指定されたユーザまたはユーザグループによるオブジェクト300の使用／アクセスに属する属性を、指定し得る。「リンク化リスト」構造中に追加的なサブジェクトレコード470を設けることにより、任意の数の異なるユーザまたはユーザグループが、アクセス制御リスト（各々は異なる属性セット472(3)を有する）に追加され得る。

サブジェクトレコードリファレンスフィールド472(4)は、ユーザ権利テーブル464内の一つ以上のレコードを参照する。図３３は、ユーザ権利テーブルレコード464(k)の、好適なフォーマットの一例を示す。ユーザ権利レコード464(k)は、URTヘッダ474、レコード権利ヘッダ476、およびユーザ選択レコード478のセットを有し得る。URTヘッダ474は、サイトレコードナンバーフィールド、URTレコード464(k)内の権利レコード数を指定するフィールド474(2)、「最初の」権利レコード（すなわち権利レコードヘッダ476）を参照するフィールド474(3)、サブジェクトテーブル462からのルックアップの有効性検査に使用されるタグ474(4)、権利レコードヘッダ476に対するルックアップの有効性検査に使用されるタグ474(5)、およびチェック値フィールド474(6)を有する。

好適な実施態様における権利レコードヘッダ476は、サイトレコードナンバーフィールド476(1)、権利IDフィールド476(2)、「次の」権利レコード476(2)を参照するフィールド476(3)、ユーザ選択レコード478(1)の最初のセットを参照するフィールド476(4)、URTヘッダタグ474(5)による有効性検査を可能にするタグ476(5)、ユーザ選択レコードタグ478(6)による有効性検査を可能にするタグ476(6)、およびチェック値フィールド476(7)を有し得る。権利IDフィールド476(2)は、例えば、権利レコード476によって伝えられる(conveyed)権利（例えば、使用する権利、配布する権利、読む権利、監査する権利など）のタイプを指定し得る。

権利レコードヘッダ476によって参照される一つ以上のユーザ選択レコード478は、対応するVDEオブジェクト300へのアクセスおよび／または使用に対応する、ユーザ選択を表示する。対応するユーザまたはユーザグループに対して承認された各権利に対して、典型的には一つの権利レコード476が存在する。これらの権利は、そのユーザまたはユーザグループによるVDEオブジェクト300の使用を支配する。例えば、ユーザは「アクセス」権利および「抽出」権利は有しても、「コピー」権利は有さないかも知れない。権利レコード476（好適な実施態様においてはREGISTERメソッドを用いてPERC808から導かれる）によって制御される他の権利には、配布権利、監査権利、および価格付け権利(pricing right)がある。オブジェクト300が電子機器600に登録され、特定のユーザまたはユーザグループに登録されたとき、ユーザは、PERC808に表示された様々な使用メソッド中からの選択を許可され得る。例えば、VDEオブジェクト300は、２つの計量方法を必要とし得る。すなわち、課金目的のための一つと、ユーザによって使用されたプロモーションマテリアルに関するデータを蓄積するためのもう一つとである。ユーザは、様々な計量／課金メソッドの選択を許され得る。例えば、VISAによる支払いか、あるいはMasterCardによる支払いか；情報データベースから検索されたマテリアルの量に基づく課金か、使用時間に基づく課金か、および／またはその両方による課金かなどである。ユーザは、そのコンテンツの検索に関するある種の詳細を第三者に提供すること（例えば人口統計学目的のために）に同意するならば、時間制および／または従量制課金において割引を受け得る。オブジェクトお

よび／またはそのオブジェクトのユーザの登録時に、ユーザは、最初に得る計量用の「アクティブな計量メソッド」として、特定の計量方法を選択するように訊ねられるであろう。VDE配布者は、ユーザ用の利用可能な選択肢の全体(universe)を、PERC808によって規定されるオリジナル選択アレイのサブセットに狭め得る。これらのユーザ選択およびコンフィギュレーション設定は、ユーザ選択レコード480(1)、480(2)、480(N)に格納される。ユーザ選択レコードは、ユーザ権利テーブル464内に明示的に述べられる必要はなく、代わりに、ユーザ選択レコード480が、特定のVDEメソッドおよび／またはそれらメソッドをパラメータ化する情報を参照する（例えばサイトリファレンスナンバーによって）ことも可能である。そのようなユーザ選択レコード480によるメソッド1000への参照は、ユーザ選択レコード内に含まれる有効性検査タグによって有効性検査されなければならない。このようにして、好適な実施態様におけるユーザ選択レコード480は、対応するVDEオブジェクト300（図２７に示すように）に使用するための一つ以上のメソッド1000を、選択し得る。これらのユーザ選択レコード480は、それ自体、メソッド1000およびメソッドを実現するための適切なコンポーネントアセンブリ690を構築するために用いられるその他の情報を、完全に定義し得る。または、ユーザ権利レコード464を参照するために用いられるユーザ／オブジェクトレコード462は、VDEオブジェクト300に対応するPERC808を参照することによって、コンポーネントアセンブリ690を構築するために必要な追加的な情報を提供したり、および／または他にもVDEオブジェクト300にアクセスし得る。例えば、PERC808は、選択されたメソッド、オブジェクトコンテンツの復号化用および／または暗

号化用の、秘密本体および／または権利鍵に属するMDE1202を得るためにアクセスされ得、また、ユーザ権利レコードが、PERC内に実現される現在の承認機構(authorization)によって承認された権利のみを伝えることを確実にするためのチェック能力を提供するためにも使用され得る。

本発明の一実施態様において、安全データベース610を格納しかつ組織化するために従来のデータベースエンジンを用いることができ、上述の暗号化層は、従来のデータベース構造の「上に」(on top of)位置してもよい。しかし、そのよ

うな従来のデータベースエンジンが、安全データベース610中のレコードを組織化して上述したセキュリティ上の考慮事項をサポートすることが不可能な場合、電子機器600が、別のインデックス化構造を暗号化形態で維持してもよい。これらの別のインデックス化構造は、SPE503によって維持することができる。この実施態様は、SPE503が、インデックスを復号化し、復号化されたインデックスブロックをサーチして適切な「サイトレコードID」その他のポインタを探すことを必要とする。次にSPE503は示されたレコードを、従来のデータベースエンジンから要求してもよい。もしレコードIDをレコードリストに対してチェックし得ない場合、SPE503は、所望のレコードを検索できるようにデータファイル自体を求めることが必要になるかもしれない。SPE503はその場合、ファイルが不正改変されていず、適正なブロックがリターンされることを確実にするために、適切な認証を行う。SPE503は、単純にインデックスを従来のデータベースエンジンに渡してはいけない（データベースエンジン自体が安全でない限り）。なぜなら、そうすることにより、要求されたレコードが不正な(incorrect)レコードに交換されることを許してしまうからである。

図３４は、上述のサイトレコードナンバーが安全データベース610内の様々なデータ構造にアクセスするために使用され得る様子の一例を示す。この例において、安全データベース610は更に、複数のサイトレコードナンバーを格納するサイトレコードテーブル482を有する。サイトレコードテーブル482は、安全データベース610内の全てのレコードのいわば「マスターリスト」を格納し得る。サイトレコードテーブル482に格納されるこれらのサイトレコードナンバーは、安全データベース610内の任意のレコードへのアクセスを可能にする。このようにして、

サイトレコードテーブル482内のサイトレコードの一部はオブジェクト登録テーブル460内のレコードをインデックスし、サイトレコードテーブル内の他のサイトレコードナンバーはユーザ／オブジェクトテーブル462内のレコードをインデックスし、サイトレコードテーブル内のさらに他のサイトレコードナンバーはURT464内のレコードにアクセスし、サイトレコードテーブル内のさらに他のサイト

レコードナンバーはPERC808にアクセスし得る。さらに、メソッドコア1000'の各々は、サイトレコードテーブル482にアクセスされ得るように、サイトレコードナンバーを有し得る。

図３４Ａは、サイトレコードテーブル482内のサイトレコード482(j)の一例を示す。サイトレコード482(j)は、レコードのタイプを示すフィールド484(1)、レコードのオーナーまたは作成者を示すフィールド484(2)、サイトレコード482(j)が指し示すレコードに関する追加的な情報を提供する「クラス」フィールド484(3)および「インスタンス」フィールド484(4)；レコードに関連する何らかの特異的なデスクリプタ（例えばオブジェクトID）を示す特異的デスクリプタフィールド484(5)；テーブルその他の、サイトレコードが参照するデータ構造の識別子(identification)484(6)；レコードが開始する場所を示す、そのデータ構造内の参照および／またはオフセット；ルックアップされているレコードの有効性検査を行うための有効性検査タグ484(8)、およびチェック値フィールド484(9)を有し得る。フィールド484(6)および484(7)は共に、サイトレコード484(j)によって参照されるレコードが実際に物理的に安全データベース610内に位置するためのメカニズムを提供し得る。

安全データベース610の更新

図３５は、情報交換所、VDE管理者またはその他VDE参加者によってエンドユーザの電子機器600に維持されている安全データベース610を更新するために使用され得るプロセス1150の一例を示す。例えば、図３５に示すプロセス1500は、安全データベース610内の「監査追跡」レコードを収集し、および／またはエンドユーザの要求に応じて新しい予算およびパーミッション（例えばPERC808）を提供するために、使用され得る。

典型的には、エンドユーザの電子機器600は、情報交換所（ブロック1152）と

通信を開始し得る。この接触(contact)は、例えば、ユーザコマンドに応答して、もしくは自動的に確立され得る。電子ハイウェイ108を介して開始されてもよく、また、他の通信ネットワークを介して、例えばLAN、WAN、双方向ケーブルまたはポータブルメディアによる交換(exchange)を行って、電子機器間で開始され得

る。管理情報の交換プロセスは、一回の「オンライン」セッション中で行われる必要はなく、ある時間にわたって、いくつかの異なる一方向および／または双方向通信に基づき、同じまたは異なる通信手段上で行われてもよい。しかし、図３５に示すプロセス1150は、エンドユーザの電子機器600およびその他のVDE参加者（例えば情報交換所）が、電話線、ネットワーク、電子ハイウェイ108などを介して双方向リアルタイムインタラクティブ通信交換を行う、具体的な例である。

エンドユーザの電子機器600は一般に、特定のVDE管理者または情報交換所に接触する。特定の情報交換所の識別は、ユーザがアクセスしたいあるいはすでにアクセスしたVDEオブジェクト300に基づく。例えば、ユーザがすでに特定のVDEオブジェクト300にアクセスし、さらなるアクセスを行うための予算を使い切ってしまったとする。ユーザは、その特定のオブジェクトに責任を有するVDE管理者、配布者および／または金融情報交換所（financial clearhouse）にユーザの電子機器600を自動的に接触させるような、要求を発することができる。接触すべき適切なVDE参加者の識別は、本例において、例えば、UDE1200、MDE1202、オブジェクト登録テーブル460および／またはサブジェクトテーブル462内の情報によって提供される。電子機器600は、複数のVDE参加者に接触しなければならないかも知れない（例えば、監査レコードをある参加者に配布し、追加的な予算その他のパーミッションを別の参加者から得るためなど）。接触1152は、一例において、図２７の発送テーブル444および図２９の管理的イベントログ442に基づいてスケジューリングされ得る。

いったん接触が確立されると、エンドユーザの電子機器および情報交換所は、典型的には、互いに認証しあい、リアルタイム情報交換で用いるセッション鍵について合意する（ブロック1154）。いったん安全な接続が確立されると、エンドユーザの電子機器は、（例えば発送テーブル444に基づいて）情報交換所に送るべき監査情報を含む管理的オブジェクトを有するものであるか否かを、決定し得る（決定ブロック1156）。いくつかのVDEオブジェクト300に属する監査情報が、同じ送信用の管理的オブジェクト内に置かれてもよいし、異なる管理的オブジェクトは異なるオブジェクトに関する監査情報を含んでいてもよい。エンドユーザ

の電子機器がこの特定の情報交換所に送るべきそのような管理的オブジェクトを少なくとも一つ有しているとすると（決定ブロック1156の「yes」出口）、電子機器は、今回確立された安全なリアルタイム通信を介して、その管理的オブジェクトを情報交換所に送る（ブロック1158）。一つの具体的例として、単一の管理的オブジェクトが、各異なるオブジェクトについての監査情報が管理的オブジェクト内の別の「イベント」を侵犯する(compromise)ような複数のVDEオブジェクトに属する監査情報を含む管理的オブジェクトとして、送られ得る。

情報交換所は、管理的オブジェクトを受信し、そのコンテンツを処理してコンテンツが「有効」(valid)で「正当」(legitimate)なものであるか否かを決定する。例えば、情報交換所は、含まれた監査情報を分析して、該当するVDEオブジェクト300の不適正使用(misuse)を示すか否かを決定する。情報交換所は、この分析の結果として、一つ以上の応答(responsive)管理的オブジェクトを生成し、そしてエンドユーザの電子機器600に送り得る（ブロック1160）。エンドユーザの電子機器600は、受信された管理的オブジェクトに基づいてその安全データベース610および／またはSPU500コンテンツを更新するイベントを、処理し得る（ブロック1162）。例えば、情報交換所が受信した監査情報が正当であれば、情報交換所は、電子機器に送信された監査情報を削除および／または圧縮することを要求する、管理的オブジェクトをエンドユーザの電子機器600に送り得る。これに代えてあるいは追加的に、情報交換所は、この段階でエンドユーザ電子機器600から追加的な情報を要求し得る（例えば初期の送信中に不正化した特定の情報の再送信、以前には送信されなかった追加的な情報の送信）。もし情報交換所が受信した監査情報に基づいて不正使用を検知した場合は、エンドユーザが関連VDEオブジェクト300にさらにアクセスする権利を取り消しその他改変する管理的オブジェクトを、送信し得る。

情報交換所は、これに代えてあるいは追加的に、エンドユーザの電子機器600に、電子機器が一つ以上のメッセージを表示するように命令する管理的オブジェクトを、送り得る。これらのメッセージは、ユーザに特定の状態(conditions)を告知し、および／またはユーザから追加的な情報を要求し得る。例えば、メッセ

ージはエンドユーザに、電話その他により情報交換所に直接接触して表示された問題を解決するように指示してPINを入力したり、またはユーザに新しいサービス会社に接触して関連VDEオブジェクトを再登録することを、指示し得る。または、メッセージは、オブジェクトに関して新しい使用許可を得る必要があることをエンドユーザに告げ、ユーザに費用、ステータスその他の関連情報を告知し得る。

同じまたは異なる通信交換中に、同じまたは異なる情報交換所が、VDEオブジェクト300に属する追加的な予算および／またはパーミッションを求めるエンドユーザの要求を、扱い得る。例えば、エンドユーザの電子機器600（例えば、特定のVDEオブジェクト300にアクセスを求めるユーザ入力要求に応答して）は、情報交換所に、アクセスを可能にするための予算および／またはその他のパーミッションを要求する、管理的オブジェクトを送り得る（ブロック1164）。上述のように、そのような要求は、一つ以上の管理的オブジェクトの形態、例えば、同じまたは異なるVDEオブジェクト300のための、複数の要求された予算および／またはその他のパーミッションに関連する複数の「イベント」を有する、単一の管理的オブジェクトで送信され得る。情報交換所は、そのような要求を受信すると、エンドユーザのクレジット、財政レコード、ビジネス契約(agreement)および／または監査履歴をチェックすることにより、要求された予算および／またはパーミッションが与えられるべきか否かを決定する。情報交換所は、この分析に基づいて、イベントユーザの電子機器600にその安全データベースを応答して更新させる、一つ以上の応答管理的オブジェクトを送り得る（ブロック1166、1168）。この更新は、例えば、失効したPERC808を新しいものにリプレースすること、追加的な（またはより少ない）権利を提供するようにPERCを改変すること、などを含み得る。ステップ1164～1168は、同じまたは異なる通信において複数回繰り返されることによって、更なる更新物をエンドユーザの安全データベース610に提供し得る。

図３６は、新ししルコードまたはエレメントが安全データベース610中に挿入

され得る様子の一例を示す。図３５に示すロードプロセス1070は、ロードされた

各データエレメントまたはアイテムを、不正改変、リプレース、あるいは置換されていないことを確実にするためチェックする。図３５に示すプロセス1070において、最初に行われるべきステップは、電子機器600の現在のユーザがアイテムを安全データベース610に挿入することを承認されているか否かをチェックすることである（ブロック1072）。このテストは、好適な実施態様において、適切なメソッド1000およびUDE1200などのその他のデータ構造をSPE503にロードすること（あるいはすでにロードされたものを使用する）によって、安全データベース610（ブロック1074）にその変更を加えることのユーザ承認を認証することを包含し得る。もしユーザが安全データベース610にその変更を行うことを承認されていることが認められれば、SPE503は、安全データベースに追加されるべきエレメントを復号化して（ブロック1076）損傷を受けたか不正化したか（ブロック1078）を決定することにより、その完全性をチェックし得る。エレメントは、所定の管理ファイル鍵(management file key)を用いて、正しく復号化されることを確かめるためにチェックされ、チェック値が有効性検査され得る。また、正しいエレメントが供給されかつ置換されていないことを確実にするため、公開および秘密ヘッダIDタグ（もし存在すれば）が比較され得、ユニークなエレメントタグIDが所定のエレメントタグに対して比較され得る。もしこれらのテストのうちいずれかに失敗すれば、エレメントは自動的に拒絶され、エラー訂正などが行われる。エレメントが完全性を有することが見いだされれば、SPE503は、例えば新しい鍵を用いて、情報を再暗号化（ブロック1080）し得る（下記の図３７の説明を参照）。同じプロセスステップにおいて、適切なタグが好ましくは提供され、情報が適切なタグを含むセキュリティラッパ(wrapper)内において暗号化される（ブロック1082）。SPE503は、適切なタグ情報を保持することにより、後にアイテムが再び安全データベース610（ブロック1084）から読まれた際に、有効性検査を行うその他によりアイテムを認証し得る。セキュリティラッパ内の今や安全となったエレメントは次に、安全データベース610内に格納され得る。

図３７は、好適な実施態様におけるデータベースで、安全データベース610に格納されたアイテムに安全にアクセスするために用いられる、プロセス1050の一

例を示す。好適な実施態様において、SPE503はまず安全データベース610レコードからのアイテムにアクセスしてこれを読み込む(read in)。SPE503は、安全データベース610からの暗号化された形態にあるこの情報を読み、SPU500のプロテクテッドメモリに内部的に格納されたアクセス鍵に基づいてこれを復号化する（ブロック1053）ことによって、「開梱(unwrap)」し得る（ブロック1052）。好適な実施態様において、この「開梱」プロセス1052は、暗号化／復号化エンジン522に、情報ブロックを管理ファイル鍵および復号化に必要なその他の必要な情報とともに送ることを、包含する。復号化エンジン522は「平文(plaintext)」情報をリターンし得、SPE503がこれをチェックすることによりオブジェクトのセキュリティが破られていなくオブジェクトが使用されるべき正しいオブジェクトであることを確実にする（ブロック1054）。読み込みエレメントが置換されていないことを確実にし他のセキュリティ上の脅威に対して保護するために、SPE503は次に、全てのコリレーションおよびアクセスタグをチェックし得る（ブロック1054）。この「チェック」プロセスの一部は、安全データベース610から得たタグを、安全なメモリまたはSPU500内に含まれるタグに対してチェックすることを包含する（ブロック1056）。SPU500内に格納されたこれらのタグは、SPUのプロテクテッドメモリからアクセスされ得（ブロック1056）、今や開梱されたオブジェクトをさらにチェックするために用いられ得る。この「チェック」プロセス1054によっても何らの不適さ(impropriety)が示されないとき（かつブロック1052もオブジェクトが不正化その他の損傷を受けていないことを示しているとき）、SPE503はアイテムにアクセスしたりその他使用する（ブロック1058）。アイテムの使用が完了すると、SPE503は、アイテムが変更されたのであればもう一度安全データベース610内に格納する必要があり得る。もしアイテムが変更されていれば、SPE503は、アイテムをその変更された形態で、暗号化のために暗号化／復号化エンジン522に送る一方、オブジェクトが適切に暗号化されるように、適切な必要情報（例えば適切な同じまたは異なる管理ファイル鍵およびデータ）を暗号化／復号化エンジンに提供する（ブロック1060）。この段階において、アイテムセキュリティラッパをユニークにタグ付けおよび／または暗号化するために、ユニークな新しいタグおよび／または暗号化鍵を用い得る（ブロック1062。図３７の詳

細な下記説明も参照）。オブジェクトが再び安全データベース610から読まれたときにSPEがオブジェクトを復号化して有効性検査を行うことができるように、SPE503は、SPU500のプロテクテッドメモリ内に鍵および／またはタグのコピーを保持してもよい（ブロック1064）。

安全データベース610レコードを復号化するための鍵は、好適な実施態様においては、SPU500のプロテクテッドメモリの中にのみ維持される。SPU500を出る各インデックスまたはレコード更新物は、タイムスタンプを受け、SPE503によって決定されるユニークな鍵によって暗号化される。例えば、レコードが次に検索されたときにどの鍵を使用すべきかをSPE503が決定できるように、安全データベース610のレコードの前に、鍵識別ナンバーを「普通に見えるように(in plain view)」置いてもよい。SPE503は、レコードまたはインデックスのサイトID、それに関連付けられた鍵識別ナンバー、およびSPE内部のリスト中の実際の鍵を維持することが可能である。ある時点で、この内部リストは満杯になるかも知れない。この時点において、SPE503は、変更された情報を含む安全データベース610内のアイテムを再暗号化する、メンテナンスルーチンをコールし得る。変更された情報を含むデータ構造中のアイテムの一部または全部が、読み込まれ、暗号化され、次に同じ鍵を用いて再復号化され得る。これらのアイテムには、その際同じ鍵識別ナンバーが発行され得る。これらのアイテムは次に、SPE503から再び安全データベース610に書き出され得る。SPE503はその後、アイテムIDおよび対応鍵識別ナンバーの内部リストをクリアし得る。次に、各新しいまたは変更されたアイテムに異なる鍵および新しい鍵識別ナンバーを割り当てるプロセスを、再び開始し得る。このプロセスを用いることにより、SPE503は、安全データベース610の（インデックスを含む）データ構造を、古いアイテムによる置換および、現在のアイテムのインデックスの置換から、保護できる。このプロセスはまた、検索されたアイテムIDを、期待されるIDの暗号化されたリストに対して、SPE503が有効性検査することを可能にする。

図３８は、このプロセスをより詳細に示すフローチャートである。安全データベース610のアイテムが更新または改変されたときは必ず、更新されたアイテムに対して新しい暗号化鍵が発生されることが可能である。新しい鍵を用いた暗号

化は、セキュリティを加え、安全データベース610レコードのバックアップコピーの不適正使用を防ぐために行われる。各更新された安全データベース610レコードの新しい暗号化鍵は、SPU500の安全なメモリ内に、該当する安全データベースレコード（単数または複数）の識別子(identification)とともに、格納され得る。

SPE503は、安全データベース610内に格納しようとする各新しいアイテムに対して、新しい暗号化／復号化鍵を発生し得る（ブロック1086）。SPE503は、この新しい鍵を、安全データベースに格納する前に暗号化するために使用し得る（ブロック1088）。SPE503は、後にレコードを読み復号化できるように、鍵を保持することを確実にする。そのような復号化鍵は、好適な実施態様において、SPU500内のプロテクトされた不揮発性メモリ（例えばNVRAM534b）中に維持される。このプロテクテッドメモリは有限サイズを有しているので、新しい鍵をプロテクテッドメモリが格納する余地がない場合があり得る。好適な実施態様において、決定ブロック1090によってこの状態についてテストする。メモリ内に新しい鍵を格納するための余地がない場合（または、メモリ中に格納された鍵の数が所定の数を越えた、タイマが切れた(expire)などの他のイベントの場合）、好適な実施態様は、使用されている暗号化／復号化鍵の数を減らす（または変える）ために安全データベース610内の他のレコードを同じ新しい鍵で再暗号化することで、これらの状況に対処する。このようにして、安全データベース610の一つ以上のアイテムが安全データベースから読まれ得（ブロック1092）、最後に格納されたときに暗号化するために使用された古い鍵を用いて、復号化され得る。好適な実施態様において、一つ以上の「古い鍵」が選択され、古い鍵を用いて暗号化された全ての安全データベースアイテムが、読まれて復号化される。これらのレコードは今度は、ブロック1086において新しいレコードのために発生された新しい鍵を用いて、再暗号化され得る（ブロック1094）。他のレコードを復号化するために用いた古い鍵は、今やSPUプロテクテッドメモリから除かれ得（ブロック1096）、新しい鍵がその場所に格納され得る（ブロック1097）。古い鍵（単数または複数）を用いて暗号化された安全データベース610内の全てのレコードが、ブロック1092で読まれ、新しい鍵を用いてブロック1904で再暗号化されたことをSPE503

が確信できない限り、古い鍵（単数または複数）は、ブロック1096によって安全メモリから除かれることはない。新しい鍵を用いて暗号化（または再暗号化）された全てのレコードは今や、安全データベース610内に格納され得る（ブロック1098）。決定ブロック1090が、SPU500プロテクテッドメモリ内に新しい鍵を格納するための余地があると決定すれば、ブロック1092、1094、1096の動作は不必要になり、SPE503は代わりに、単に新しい鍵をプロテクテッドメモリ内に格納し（ブロック1097）、新しく暗号化されたレコードを安全データベース610内に格納し得る（ブロック1098）。

安全データベース610のファイルのセキュリティは、レコードを「区画（compartment）」に細分化することにより、さらに改善され得る。異なる「区画」を保護するために、異なる暗号化／復号化鍵を用い得る。この戦略は、安全データベース610中の単一の鍵で暗号化される情報の量を制限するために、用いることが可能である。安全データベース610のセキュリティを増すための別の技術は、同一レコードの異なる部分を異なる鍵を用いて暗号化することにより、これらのレコードを復号化するために一つ以上の鍵が必要になるようにすることである。

安全データベース610のバックアップ

好適な実施態様における安全データベース610は、安全データベースが含む情報を保護するために、周期的（periodic）その他の時間間隔でバックアップされる。この安全データベース情報は、多くのVDE参加者にとって実質的な価値がある。安全データベース610のバックアップは、ユーザにとって大きな不便さを感じさせないようになされなければならず、また、いかなるセキュリティ違反になってもいけない。

安全データベース610をバックアップする必要は、電子機器600のパワーオンの際、SPE503が最初に呼ばれた（invoke）された際、周期的時間間隔、およびSPE503に維持される「監査ロールアップ」値その他の簡略（summary）サービス情報が、ユーザ設定その他のしきいを越えた場合、または一つ以上のコンテンツ出版者（publisher）および／または配布者および／または情報交換所サービスプロバイダおよび／またはユーザによって確立される条件によって誘因（trigger）される場

合に、チェックされ得る。ユーザは、ある時点までにバックアップしていない場合、またはある期間または使用量後にバックアップするように促され得る。あるいは、バックアップは、ユーザの介入なしに自動的に進められてもよい。

図８を参照して、バックアップ格納部668および格納媒体670（例えば磁気テープ）を用いてバックアップ情報を格納してもよい。勿論、任意の不揮発性媒体（例えば一つ以上のフロッピーディスク、書き込み可能光学ディスク、ハードドライブなど）をバックアップ格納部668に用いてもよい。

安全データベース610をバックアップするために、少なくとも２つのシナリオがある。第１のシナリオは「サイト特異的」であり、SPU500のセキュリティを用いてバックアップ情報の復元（restore）をサポートするものである。この第１の方法は、例えば２次的格納装置（secondary storage device）652の故障、ユーザ過失によるファイル損傷その他の、安全データベース610一部または全部損傷または不正化するような出来事により、安全データベース610に損傷があった場合に用いられる。この第１のサイト特異的バックアップシナリオは、SPU500が依然として正しく機能し、バックアップ情報を復元するために利用可能であることを想定している。

第２のバックアップシナリオは、ユーザのSPU500がもはや動作不能であり、取り替えられる必要があるかすでに取り替えられたことを想定している。この第２のアプローチは、重要データの損失を防ぐためおよび／またはユーザがエラーから回復する（recover）ことを助けるために、承認されたVDE管理者その他の承認されたVDE参加者が、格納されたバックアップ情報にアクセスすることを可能にする。

これらの両シナリオとも、図３９に示すROS602によって行われるプログラム制御ステップ例によって提供される。図３９は、安全データベース610（およびその他の情報）をバックアップ格納部668にバックアップするために電子機器600によって行われる、バックアップルーチン1250の一例を示す。バックアップが開始されると、上述のように、バックアップルーチン1250は、一つ以上のバックアップ鍵を発生する（ブロック1252）。バックアップルーチン1250は次に、全ての安全データベースアイテムを読み、安全データベース610に格納される前に、暗号

化に用いられた元の鍵を用いて各アイテムを復号化する（ブロック1254）。典型的には、SPU500が、安全データベース610のインスタンス内のこの情報を復号化するための鍵が格納される唯一の場所であるので、またバックアップルーチン1250によって提供されるシナリオの一つはSPU500が完全に故障したか破壊された場合であるので、バックアップルーチン1250は、バックアップからの回復がSPU内のこれらの鍵の知識に依存しないように、この読みおよび復号化ステップ1254を行う。むしろ、バックアップルーチン1250は、新しく発生されたバックアップ鍵（単数または複数）を用いて各安全データベース610アイテムを暗号化し（ブロック1256）、暗号化されたアイテムをバックアップ格納部668に書き戻す（ブロック1258）。このプロセスは、安全データベース610中の全てのアイテムが読まれ、復号化され、新しく発生されたバックアップ鍵（単数または複数）を用いて暗号化され、バックアップ格納部に書き戻されるまで、続けられる（決定ブロック1260によってそのテストを行う）。

好適な実施態様はまた、SPU500のプロテクテッドメモリ内にSPE簡略サービスマネージャ560によって格納された簡略サービス監査情報を読み、この情報を新しく発生されたバックアップ鍵（単数または複数）を用いて暗号化し、この簡略サービス情報をバックアップ格納部668に書く（ブロック1262）。

最後に、バックアップルーチン1250は、ブロック1252で発生されブロック1256、1262での暗号化に用いられたバックアップ鍵（単数または複数）を、バックアップ格納部668にセーブする。上述した復元シナリオの両方をカバーするために、バックアップルーチン1250は、これを、２つの安全な方法で行う。バックアップルーチン1250は、バックアップ鍵（単数または複数）を（バックアップ時刻などの他の情報および、バックアップを識別するための他の適切な情報とともに）、SPU500のみが復号化し得るようなさらなる鍵（単数または複数）を用いて、暗号化し得る。この暗号化された情報は、次にバックアップ格納部668に書き込まれる（ブロック1264）。例えば、このステップは、SPU500のみが対応する秘密鍵を知る、一つ以上の公開鍵を用いた、複数の暗号化を含み得る。または、SPU500によって発生され、SPUによってのみ保持される第２のバップアップ鍵が、公開鍵の代わりに最終暗号化のために使用され得る。バックアップ鍵を保護するために

も

ちいられる暗号化を「クラック(crack)」することによってバックアップのセキュリティを攻撃することを困難にするために、ブロック1264は複数の暗号化を含むことが好ましい。ブロック1262は暗号化された簡略サービス情報をバックアップ上に有するが、SPU装置秘密鍵、共有鍵、SPUコードその他の内部セキュリティ情報を有さないことが好ましい。これらの情報が、暗号化形態であっても決してユーザに入手可能にならないようにするためである。

ブロック1264に格納された情報は、バックアップルーチン1250を行った（または少なくとも一部行った）同じSPU500がバックアップ情報を回復するために、十分である。しかし、この情報はこの同じSPU500以外にとっては役に立たない。なぜなら、このSPUのみがバックアップ鍵を保護するために用いられる特定の鍵を知っているからである。SPU500が回復不能な故障をしてしまう他方の可能なシナリオをカバーするために、承認されたVDE管理者によって読まれ得る一つ以上のさらなる鍵のセットのプロテクション下で、バックアップ鍵（単数または複数）をセーブする追加的なステップ（ブロック1266）を、バックアップルーチン1250は提供する。例えば、ブロック1266は、バックアップ鍵を、SPU500の初期化(initialization)中にVDE管理者から受信された「ダウンロード承認鍵」を用いて、暗号化し得る。この暗号化されたバージョンの鍵はまた、格納部668に書き戻される（ブロック1266）。これはSPU500の故障時のバックアップファイルの復元をサポートするために使用され得る。すなわち、ブロック1266で用いられる「ダウンロード承認（またはその他の）鍵（単数または複数）」を知るVDE管理者は、バックアップ格納部668中のバックアップ鍵（単数または複数）を回復することができ得、続いてバックアップ安全データベース610を同じまたは異なる電子機器600に復元し得る。

好適な実施態様において、ルーチン1250によってバックアップファイル中にセーブされた情報は、承認されたVDE管理者からバックアップ承認を受信された後のみ、復元され得る。

ほとんどの場合、復元プロセスは単に、バックアップが起こってからの使用を

考慮した若干の調整とともに、安全データベース610を復元することである。これは、ユーザがさらなるプロバイダに接触して監査および課金データを送信してもらい、最後のバックアップからの行動を反映する新しい予算を受信することを、必要とし得る。最も最近の使用行動を決定または見積もる(estimate)するために、SPU500内に維持されている現在の簡略サービス情報が、バックアップ上に格納された簡略サービス情報と比較され得る。

SPU500の故障の場合には、代替(replacement)SPU500を初期化するためおよびバックアップファイルを復号化するために、承認されたVDE管理者に接触しなければならない。これらのプロセスは、SPU故障および新しいSPUへの更新の両方を可能にする。復元の場合には、ユーザのシステムに必要な情報を復元するためにバックアップファイルが使用される。更新の場合には、バックアップファイルは、更新プロセスを有効性検査するために使用され得る。

バックアップファイルは、場合によっては、電子機器600間の管理情報(management information)の送信に、使用され得る。しかし、好適な実施態様では、一部または全部の情報を、適切な承認により、電子機器間で輸送可能にすることを制限し得る。バックアップファイルの一部または全部を管理的オブジェクト内にパッケージし、分析、輸送、その他の使用のために送信され得る。

バックアップファイルからの復元を必要とするもののより詳細な例として、電子機器600が、安全データベース610の一部または全部を消去(wipe out)または不正化するようなハードディスク故障その他の事故に遭ったが、SPU500は依然として機能可能であると仮定する。SPU500は、安全データベース610を復元するために必要な全ての情報（例えば秘密鍵(secret key)その他）を含み得る。しかし、VDE管理者から復元承認が受信されるまで、ROS602が安全データベースの復元を禁止(prevent)し得る。復元承認は、例えば、SPE503が期待する値にマッチしなければならない「秘密値」を有していてもよい。VDE管理者は、所望であれば、この復元承認の提供を、例えばSPU500内に格納された簡略サービス情報が分析のため管理的オブジェクトに入れられて管理者に送信された後でのみ、初めて行うようにしてもよい。ある状況下においては、VDE管理者は、ユーザによる不正行

動(fraudulent activity)の痕跡をチェックするために、バックアップファイルの（部分的または完全な）コピーが管理的オブジェクトに入ってVDE管理者に送信されることを、要求し得る。復元プロセスは、いったん承認されると、上述のように、最終バックアップからの行動を反映するように、復元された予算レコードを調節することなどを、必要とし得る。

図４０は、安全データベース610を図３８に示すルーチンによって提供されるバックアップに基づいて復元するための、電子機器600によって行われるプログラム制御された「復元」ルーチン1268の、一例を示す。この復元は、例えば、電子機器600が故障したが、例えばVDE管理者に接触することによって回復または「再初期化」可能である場合に、使用され得る。好適な実施態様では、VDE管理者によって承認されない限りまた承認されるまでは、SPU500がバックアップから復元を行うことを許可しないため、復元ルーチン1268は、復元を行うことを承認することが可能なVDE管理者と安全な通信を確立することから、開始する（ブロック1270）。いったんSPU500とVDE管理者が互いを認証すると（ブロック1270の一部）、VDE管理者は、「進行中の作業(work in progress)」および簡略値をSPU500の内部不揮発性メモリから抽出し得る（ブロック1272）。VDE管理者は、この抽出された情報を、例えば、セキュリティ違反があったか否かを決定することを助けるために使用し得、また、故障したSPU500がそのコンテンツを効果的にVDE管理者に「ダンプ」することによって、VDE管理者がコンテンツを扱うことを可能にすることを許可する。SPU500は、この情報を暗号化して一つ以上の管理的オブジェクト中にパッケージし、VDE管理者に供給し得る。VDE管理者は次に、安全データベース610の現バックアップの一部または全部のコピーをSPU500から要求し得る(ブロック1274)。この情報は、SPU500によって、例えば一つ以上の管理的オブジェクトにパッケージし、VDE管理者に送られ得る。情報を受信するとVDE管理者は、簡略サービス監査情報をバックアップボリューム（すなわち図３８のブロック1262で格納された情報）から読むことにより、バックアップ時に格納された簡略値およびその他の情報を、決定し得る。VDE管理者はまた、図３８のブロック1264で格納された情報を読むことにより、バックアップがなされた時刻および

日付を決定し得る。

VDE管理者は、この時点において、ブロック1272およびバックアップから得られた情報に基づき、簡略値およびその他の情報を復元し得る（ブロック1276）。例えば、VDE管理者は、SPUの内部簡略値およびカウンタをリセットして、最終バックアップと一致するようにし得る。これらの値は、ブロック1272において回復された「進行中の作業」、バックアップから経過した時間量などに基づき、VDE管理者によって調整され得る。目的は典型的には、故障が起こらなければ取られたであろう値に等しい内部SPU値を、提供しようとすることにある。

VDE管理者は次に、SPU500が、バックアップファイルから安全データベース610を回復することを承認し得る（ブロック1278）。この復元プロセスは、全ての安全データベース610レコードを、バックアップからのレコードでリプレースする。VDE管理者は、これらのレコードを必要に応じて、復元プロセス中または後でSPU500にコマンドを渡すことによって、調整し得る。

VDE管理者は次に、回復された値に基づいて請求書(bill)を計算し（ブロック1280）、SPUダウンタイムから回復するためのその他の行動をとる（ブロック1282）。典型的には、目的は、ユーザに課金し、故障した電子機器600に属する他のVDE100値を、最終バックアップ以降だが故障以前に起こった使用に関して、調整することである。このプロセスは、VDE管理者が、故障以前の電子機器の使用に属する報告その他の情報を他のVDE管理者から得て、これを安全データベースバックアップと比較することにより、どの使用およびその他のイベントが未だ考慮されていないかを決定することを、包含する。

別の実施態様において、SPU500は、安全データベース610の一部または全部を格納することを可能にするのに十分な、内部不揮発性を有し得る。この実施態様において、複数の集積回路要素を含む例えば不正改変不可能な金属容器または何らかのチップパック形態などの、安全なエンクロージャ内に含まれ得る一つ以上の追加的な集積回路を用いて、不正改変の試みの防止および／または証拠となり、ならびに／または不正改変の際にSPU500または関連する重要鍵および／またはその他の制御情報を使用禁止にする(disable)ことによって、追加的なメモリが

提供され得る。図３８に示す同じバックアップルーチン1250がこのタイプの情報をバックアップするために使用され得る。唯一の相違点は、ブロック1254は安全データベースアイテムをSPUの内部メモリから読み得、バックアップ鍵を用いて暗号化する以前に復号化することが不必要であり得ることである。

イベント駆動型(event-driven)VDEプロセス

上述のように、好適な実施態様による／おける権利オペレーティングシステム(ROS)602は、「イベント駆動型」であり得る。この「イベント駆動型」能力は、集積化および拡張性を容易にする。

「イベント」は、任意の時刻における出来事である。「イベント」の例としては、ユーザがキーボードのキーを打鍵することや、メッセージまたはオブジェクト300が到着すること、タイマーが切れること、または、別のプロセスからの要求などがある。

好適な実施態様において、ROS602は「イベント」に応えてプロセスを行うことによって、「イベント」に応答する。ROS602は、イベントの発生に応答して、アクティブプロセスおよびタスクを動的に作成する。例えば、ROS602は、一つ以上のコンポーネントアセンブリ690を作成し、イベントの発生に応答して単数または複数のプロセスを行うようにその実行を開始し得る。アクティブプロセスおよびタスクは、ROS602がイベントに応答した時点で、終了し得る。この、イベントに応答して動的にタスクを作成する（また終了する）能力は、大きな柔軟性を提供し、また、例えばSPU500によって提供されるような有限の実行リソースで、実質的に無限の多様な異なるプロセスを、異なる文脈で行うことを可能にする。

「イベント」はあるゆるタイプの出来事であり得るので、無限の異なるイベントがある。従って、イベントを異なるタイプにカテゴリー化するどのような試みも、概括に過ぎない。これを念頭に置きながら、好適な実施態様によって提供／サポートされるイベントを、２つの広いカテゴリーに分類することができる：

・ユーザ開始型イベント、および

・システム開始型イベント、である。

一般に、「ユーザ開始型」イベントは、ユーザ（またはユーザアプリケーショ

ン）に帰せられる出来事である。よく見られる「ユーザ開始型」イベントは、ユーザによる、オブジェクト300その他のVDE保護された情報にアクセスしたいという、要求（例えばキーボードのボタンを押下すること、またはリダイレクタ684を透過的に用いることによる）である。

「システム開始型」イベントは、一般に、ユーザに帰せられない出来事である。システム開始型イベントの例としては、情報が不揮発性メモリにバックアップされなければならないことを示すタイマーが切れること、別の電子機器600からのメッセージの受信、および別のプロセス（システム開始型イベントおよび／またはユーザ開始型に応答するように開始されたかも知れない）によって発生されるサービスコールなどである。

好適な実施態様で提供されるROS602は、イベントを処理するためのプロセスを指定して開始することによって、イベントに応答する。これらのプロセスは、好適な実施態様において、メソッド1000に基づく。無限の異なるタイプのイベントがあるため、好適な実施態様は、イベントを処理するための無限の異なるプロセスをサポートする。この柔軟性は、例えばメソッドコア1000'、ロードモジュール1100、およびUDE1200などのデータ構造といった独立的に配送可能なモジュールから、コンポーネントアセンブリを動的に作成することによってサポートされる。好適な実施態様によってサポート／提供される無限の潜在的なプロセスタイプをどのようにカテゴリー化しても概括でしかないが、プロセスは、以下の２つのカテゴリーに概して分類可能である：

・VDE保護された情報の使用に関連するプロセス、および

・VDE管理に関連するプロセス、である。

「使用」および「管理的」プロセス

「使用」プロセスは、VDE保護された情報の使用に何らかの関係を有する。好適な実施態様で提供されるメソッド1000は、VDE保護された情報の使用についての制御チェーンを作成し維持するプロセスを、提供し得る。「使用」タイプのプロセスの一つの具体例は、ユーザが、VDEオブジェクト300を開いてそのコンテンツにアクセスすることを許可するプロセスである。メソッド1000は、詳細な使用

関連プロセス、例えばコンテンツの要求に応じた（許可された場合）ユーザへの放出、および計量、予算、監査追跡の更新など、を提供し得る。使用関連プロセスはユーザ開始型であることが多いが、使用プロセスの一部は、システム開始型であり得る。VDE使用関連プロセスを誘起する(trigger)イベントを、「使用イベント」と呼び得る。

「管理的」プロセスは、VDE100が機能し続けることを助けるものであり、VDE100を安全かつ効率的に動作させ続ける、取引管理(management)「インフラストクラクチャ」をサポートすることを助ける処理を、提供する。管理的プロセスは、例えば、VDEの処理および制御チェーンを確立し維持する、VDE保護されたデータ構造の作成、改変および／または破棄のある側面に関連する、処理を提供し得る。例えば、「管理的」プロセスは、VDE電子機器600の安全データベース610内に含まれる情報を格納、更新、改変、または破棄し得る。管理的プロセスはまた、異なるVDE電子機器600間の安全な通信を、確立、維持およびサポートする通信サービスを提供し得る。管理的プロセスを誘起するイベントを、「管理的イベント」と呼び得る。

相互的メソッド(reciprocal method)

一部のVDEプロセスは、それらが互いに相互作用しあう様子に基づいて、対にされる。あるVDEプロセスは、別のVDEプロセスからの処理サービスを「要求」し得る。処理サービスを要求するプロセスを、「要求プロセス」と呼び得る。「要求」は、対の中の他方のVDEプロセスによる処理を誘起するため、「イベント」である。「要求イベント」に応答するVDEプロセスは、「応答プロセス」と呼び得る。「要求プロセス」および「応答プロセス」を、「相互的プロセス」と呼び得る。

「要求イベント」は、例えば、一つのVDEノード電子機器600から発行されるメッセージまたは、ある情報のためのプロセスを有し得る。対応する「応答プロセス」は、例えばメッセージ中で要求された情報を送ることによって、「要求イベント」に応答し得る。この応答自体、さらなるVDE「応答プロセス」を誘起するならば、「要求イベント」であり得る。例えば、先に発生した要求に応答するメ

ッセージを受信することは、「返答(reply)プロセス」を誘起し得る。この「返答プロセス」は、別の「応答プロセス」からの「返答」に応答して誘起される、特殊なタイプの「応答プロセス」である。所与のVDE取引中において、任意の数の「要求」および「応答」プロセスの対があり得る。

「要求プロセス」およびその対になる「応答プロセス」は同じVDE電子機器600上で行われてもよく、また、これら２つのプロセスは、異なるVDE電子機器上で行われてもよい。対をなす２つのプロセス間の通信は、安全な（VDE保護された）通信、「チャネル外(out of channel)」通信、またはその２つの組み合わせによってなされてもよい。

図４１ａ～４１ｄは、処理および制御チェーンが「相互的メソッド」を用いて可能にされる様子を示す１組の例である。処理および制御チェーンは、その一部分、要求－応答式に協力する「相互的イベント」の一つ以上の対を用いて構築される。好適な実施態様において、一つ以上の「相互的メソッド」において相互的イベントの対が管理（manage）され得る。上述のように、「相互的メソッド」は、一つ以上の「相互的イベント」に応答し得るメソッド1000である。相互的メソッドは、物理的および／または時間的に離れたVDEノードにおいて、安全に実行され得る協力するプロセスの２つの半分を、含む。相互的プロセスは、柔軟に定義された情報渡しプロトコル(information passing protocol)および情報コンテンツ構造を有し得る。相互的メソッドは実際、同じまたは異なるVDEノード600上で動作する、同じまたは異なるメソッドコア1000'に基づき得る。図４１ａに示すVDEノード600Aおよび600Bは、同一の物理的な電子機器600または、別々の電子機器であってもよい。

図４１ａは、一対の相互的イベントの動作の一例を示す。VDEノード600Aにおいて、メソッド1000aは、VDEノード600Bで処理されなければならない要求を有するイベントを処理している。この「要求」イベントに応答するメソッド1000a（例えば、関連ロードモジュール1100およびデータを含むコンポーネントアセンブリ690に基づく）を、図４１ａにおいて1450として示す。プロセス1450は、要求(1452)および、オプションとして、他方のVDEノード1000bに送られて相互的イベントに関連づけられたプロセスによって処理される何らかの情報またはデータ

を作成する。要求およびその他の情報は、本明細書で他記した任意の輸送メカニズムによって、送信され得る。

VDEノード600bによる要求の受信は、そのノードにおける応答イベントを包含する。要求の受信に際して、VDEノード600bは、同じまたは異なる方法1000bによって定義される「相互的」プロセス1454を行うことにより、応答イベントに応答し得る。相互的プロセス1454は、コンポーネントアセンブリ690（例えば、一つ以上のロードモジュール1100、データ、およびオプションとして、VDEノード600B中に存在するその他のメソッド）に基づき得る。

図４１ｂは、図４１ａに示したコンセプトを、VDEノード600BからVDEノード600Aへと戻る応答を含むように、拡張したものである。図４１ａに示したように、要求イベントおよび情報である1452の、VDEノード600B中の応答プロセス1454による受信および処理によって、プロセスは、開始する。応答プロセス1454は、その処理の一部として、別の要求プロセス(1468)と協力して、応答1469を開始VDEノード600Aに送り返す。メソッド1000Aによって提供される、対応する相互的プロセス1470は、この要求イベント1469に応答し、これを処理し得る。このようにして、２つ以上のVDEノード600A、600Bは、協力してコンフィギュレーション可能な情報および要求を、ノードにおいて実行しているメソッド1000A、1000B間で渡す。第１および第２の要求－応答シーケンス［（1450、1452、1454）および（1468、1469、1470）］は、時間的および空間的距離によって隔たれ得る。効率性のために、要求（1468）および応答（1454）プロセスは、同じメソッド1000上に基づいても、同じまたは異なるメソッドコア1000'中の２つのメソッドとして実現されてもよい。メソッド1000は、異なるイベントに対して異なる振る舞い／結果を提供するように、あるいは異なるメソッドが異なるイベントに対して提供されるように、「イベントコード」によってパラメータ化され得る。

図４１ｃは、図４１ａ～４１ｂ制御メカニズムの３つのノード（600A、600B、600C）への拡張(extension)を示している。各要求－応答対は、図４１ｂで説明したように動作し、いくつかの対は互いにリンクされて、数個のVDEノード600A、600B、600Cの間に、制御および処理チェーンを形成する。このメカニズムは、制御および処理チェーンを、任意のコンフィギュレーションのノードを使用した

任

意の数のVDEノードに拡張するために、用い得る。例えば、VDEノード600Cは、VDEノード600Aに直接通信し、VDE600Bに直接通信してもよい。VDE600Bはそれ自体、VDEノード600Aに通信する。または、VDEノード600CがVDEノード600Aと直接通信し、VDEノード600AがVDEノード600Bと通信し、VDEノード600BがVDEノード600Cと通信してもよい。

メソッド1000は、関連的または協力的(related or cooperative)機能を指定する、イベントのセットによってパラメータ化し得る。イベントは、機能によって論理的にグループ分けされてもよく（例えば、使用、配布など）、また、互いと協力して(in conjunction with each other)動作し得るプロセスを指定する相互的イベントのセットでもよい。図４１ｄは、予算の配布をサポートする、コンテンツ配布モデル中の、数個のVDEノード102、106、112間の協力的処理をサポートする「相互的イベント」のセットを図示している。本例における処理および制御チェーンは、BUDGETメソッド内で指定される「相互的イベント」のセットを用いて可能にされる。図４１ｄは、例示のBUDGETメソッド（1510）内での相互的イベントの振る舞いが、協力して作動し、数個のVDEノード間の処理および制御チェーンを確立する様子を示している。本例のBUDGETメソッド1510は、プロセスが予算付けされるメカニズムを定義する「使用」プロセス1476を行うことによって、「使用」イベント1478に応答する。BUDGETメソッド1510は、例えば、計量カウントを予算値と比較し、計量カウントが予算値を越えていれば動作を中止させる(fail)、使用プロセス1476を指定し得る。また、前記BUDGET決定の結果を記載する監査追跡を、書き込み得る。予算メソッド1510は、予算のさらなる配布のためのプロセスおよび／または制御情報を定義する、配布プロセス1472を行うことにより、「配布」イベントに応答し得る。「要求」イベント1480には、ユーザが配布者からの配布権利および／または使用をどのように要求し得るかを指定する、要求プロセス1480を行うことによって、応答し得る。「応答」イベント1482には、配布者が、その予算の一部（または全部）を配布した他のユーザからの要求に応答する方法を、指定する応答プロセス1484を行うことによって、応答し得る。「

返答」イベント1474には、（より多くの）予算を再賦与または否定するメッセージにユーザがどのように応答すべきかを指定する、返答プロセス1475を行うことによって、応答し得る。

好適な実施態様において、イベント処理、相互的イベント、ならびにその関連メソッドおよびメソッドコンポーネントの制御は、PERC808によって提供される。これらのPERC(808)は、データ構造の作成、改変および配布を支配する管理的メソッドおよび、これらのアイテムのアクセス、改変およびさらなる配布を許可する管理的メソッドを参照し得る。このようにして、処理および制御チェーン中の各リンクは、例えば、監査情報をカスタマイズし、コンテンツを使用するための予算要件を変更し、および／またはこれらの権利のさらなる配布を、配布チェーン上の先行メンバー（要素）によって指定された方法で制御する能力を、有し得る。

図４１ｄに示す例において、VDE配布者ノード（106）の配布者は、別のノード（102）のコンテンツ作成者から、予算を要求し得る。この要求は、安全VDE通信の文脈でなされるかも知れないし、また、「チャネル外」通信（例えば電話または手紙により）において渡されるかも知れない。作成者102は、予算を配布者106に賦与することを決定し得、配布イベント（VDEノード102のBUDGETメソッド1510中の1452）を処理する。BUDGETメソッド中のこの配布イベントを処理する結果として、使用および再配布権利を賦与する予算が作成者102から配布者に送信され得るような安全な通信（1454）が、VDEノード102および106間に、得られ得る。配布者のVDEノード106は、予算情報の受信に対して、BUDGETメソッド1510の返答プロセス1475Bを用いて通信を処理することによって、応答し得る。返答イベント処理1475Bは例えば、配布者VDE106ノード内に予算およびPERC808をインストールして、アクセスが少なくとも部分的には予算および／またはPERCによって制御されるコンテンツまたはプロセスに、配布者がアクセスすることを可能にする。ある時点において、配布者106はまた、配布者106がアクセス権利を賦与されたコンテンツを使用することを望み得る。

コンテンツオブジェクトの使用を登録後、ユーザ112は、使用プロセスの一環

としてコンテンツオブジェクトを例えば開き、読み、書き、および／または閉じるために、「使用」プロセス1476Cのアレイを利用することを必要とすることになるだろう。

配布者106は、その予算の全部を使い切ってしまうと、追加的な予算を得ることを所望し得る。その場合、配布者106は、BUDGETメソッド要求プロセス（1480B）を用いるプロセスを、開始し得る。要求プロセス1480Bは、コンテンツ作成者VDEノード102と、より多くの予算およびもしかしたら今日までの使用行動の詳細（例えば監査追跡）を提供することを要求して、通信（1482AB）を開始し得る。コンテンツ作成者102は、作成者のBUDGETメソッド1510A内の応答プロセス（1484A）を用いて、「より多くの予算を得る」要求イベント1482ABを処理する。応答プロセス1484Aは、例えば、使用情報がコンテンツの正しい使用を示し、および／または配布者がより多くの予算に値するほど信頼に足るか否かを決定し得る。BUDGETメソッド応答プロセス1484Aはまた、上記使用についての支払いのために配布者からファンドを送信するための金融取引を開始するか、配布プロセス1472Aを用いて予算を配布者106に配布し得る。より多くの予算を賦与する（またはより多くの予算を否定する）配布者106への応答は、要求通信1482ABへの応答として直ちに送られるか、別の通信の一環として後に送られ得る。応答通信は、配布者のVDEノード106で受信されると、BUDGETメソッド1510Bの配布者が有するコピー内の返答プロセス1475Bを用いて、処理され得る。返答プロセス1475Bは次に、追加的な予算を上述と同じように処理し得る。

処理および制御チェーンは、予算情報を掲示(post)することに加え、上記予算を利用する方法を支配する制御情報も、渡し得る。例えば、上記例において指定されている制御情報はまた、配布者による作成者のコンテンツオブジェクトを使用する権利の再配布に適用される、プロセスおよび制限を記述する、制御情報を含み得る。このように、BUDGETメソッド1510Bの配布者が有するコピー内の配布プロセス1472Bを用いて配布者がユーザからの予算要求に応答するとき（上述のVDEノード106と102との間の通信と同様の性質である、VDEノード112のユーザVDEとノード106の配布者との間の通信）、上述のものと同様の配布および要求／応

答／返答プロセスが開始され得る。

このように、本例において、単一のメソッドによって、異なる「誘起」イベントに基づいた複数の動的な振る舞いが得られる。例えば、単一のBUDGETメソッド1510で、下記に挙げるイベントの任意のものあるいは全てをサポートし得る：

イベントタイプ	イベント	プロセス説明
「使用」イベント	予算を使用	予算を使用。
ユーザノード要求プロセス1480cによって処理される要求イベント	より多くの予算の要求	より大きな金額を予算として要求。
	監査者＃１による監査の要求	監査者＃１による予算使用の監査を要求。
	予算削除の要求	予算をシステムから削除することを要求。
	メソッド更新を要求	監査に使用されるメソッドを更新。
	監査者の変更要求	監査者１から監査者２へ変更、またはその逆。
	異なる監査インターバルの要求	監査間の時間インターバルを変更。
	予算コピーを提供する能力の要求	予算のコピーを提供する能力を要求。
	予算を分配する能力の要求	予算を他のユーザに分配する能力の要求。
	アカウントステータスの要求	アカウントの現ステータスに関する情報の要求。
	新しいメソッドの要求	新しいメソッドを要求。
	メソッド更新の要求	メソッドの更新を要求。
	メソッド削除の要求	メソッドの削除を要求。
ユーザノード要求プロセス1480Cによって処理される応答イベント	より多くの予算を受け取る	より大きな金額を予算に割り当てる
	メソッドの更新物を受け取る	メソッドを更新する。

	監査変更を受け取る	ある監査者から別の監査者へ変更。
	監査インターバルの変更を受け取る	監査間のインターバルを変更。
	予算削除を受け取る	予算を削除。
	監査者＃１に監査を提供	監査者＃１に監査情報を与える。
	監査者＃２に監査を提供	監査者＃２に監査情報を与える。
	アカウントステータスを受け取る	アカウントステータスを提供。
	新規を受け取る	新しい予算を受け取る。
	メソッド更新物を受け取る	更新された情報を受け取る。
	より多くを受け取る	より多くを予算として受け取る。
	監査を送る	監査情報を送る。
	削除を行う	情報を削除する。
「配布」イベント	新規作成	新しい予算を作成。
	より多くを提供	より多くを予算として提供。
	監査	監査を行う。
	削除	情報を削除する。
	調和	予算と監査とを調和させる。
	コピー	予算をコピー。
	配布	予算を配布。
	メソッド改変	メソッドを改変する。

	表示メソッド	要求されたメソッドを表示する。
配布者ノード要求プロセス1484Bによって処理される「要求」イベント	削除	情報を削除する。
	新規を得る	新しい予算を得る。
	より多くを得る	より多くを予算として得る。
	更新される	更新された情報を得る。
	監査される	監査情報を得る。
配布者ノード要求プロセス1484Bによって処理される「応答イベント」	新規をユーザに提供	新らしい予算をユーザに提供。
	より多くをユーザに提供	より多くの予算をユーザに提供
	更新物をユーザに提供	更新された予算をユーザに提供
	ユーザを監査	指定されたユーザを監査。
	ユーザのメソッドを削除	ユーザに属するメソッドを削除。

相互的メソッドプロセスの例

Ａ．予算

図４２ａ、４２ｂ、４２ｃおよび４２ｄはそれぞれ、好適な実施態様で提供されるBUDGETメソッド2250の代表例で行われる、プロセス制御ステップ例を示すフローチャートである。好適な実施態様において、BUDGETメソッド2250は、以下の４つの異なるモードのいずれかで動作し得る：

・使用（図４２ａ）

・管理的要求（図４２ｂ）

・管理的応答（図４２ｃ）

・管理的返答（図４２ｄ）

一般に、BUDGETメソッド2250の「使用」モードは、オブジェクトまたはそのコ

ンテンツの使用に関係するイベントに応答して、呼び出される。BUDGETメソッド2250の「管理的要求」モードは、VDE金融プロバイダと接触する必要のある何らかのユーザ行動に応答してユーザによってあるいはユーザのために呼び出され、そのタスクは基本的に、管理的要求をVDE金融プロバイダに送ることである。BUDGETメソッド2250の「管理的応答」モードは、図４２ｂのBUDGETメソッド2250の「管理的要求」の呼び出しによってVDEノードからVDE金融プロバイダへ送られた管理的要求の受信に応答して、VDE金融プロバイダにおいて行われる。BUDGETメソッド2250の「管理的応答」の呼び出しの結果として、VDE金融プロバイダからVDEユーザノードに管理的オブジェクトが送信される。最後に、図４２ｂのBUDGETメソッド2250の「管理的返答」の呼び出しが、図４２ｃに示すメソッドの「管理的応答」呼び出しによって送られた管理的要求の受信に応答して、ユーザVDEノードにおいて行われる。

好適な実施態様において、同じBUDGETメソッド2250が、図４２ａ～４２ｄに示す４つの異なるステップシーケンスの各々を行う。好適な実施態様において、異なるイベントコードがBUDGETメソッド2250に渡されることにより、これらの様々な異なるモードを呼び出され得る。勿論、４つの異なる「動的人格(dynamic personalities)」を有する単一のBUDGETメソッドの代わりに、４つの別々のBUDGETメソッドを使用することも可能であるが、好適な実施態様において、同じBUDGETメソッドをこれら４つのタイプの呼び出しの各々に用いることにより、特定の効果が得られる。

図４２ａを見て、BUDGETメソッド2250の「使用」呼び出しはまず、予算監査追跡（ブロック2252、2254）を用意(prime)し、次に予算UDEのためのDTDを得る。これは、予算UDEを得て読むために用いられる（ブロック2256～2262）。この「使用」呼び出しにおけるBUDGETメソッド2250は次に、予算監査日が切れたか否かを決定し、もし切れていたらこれを終了する(terminate)（決定ブロック2264の「yes」出口、ブロック2266、2268）。予算監査日が切れていない限り、メソッドは次に、原子エレメントおよびイベントカウントを用いて（他の情報も用いるか可能性がある）予算を更新し得（ブロック2270、2272）、次に予算ユーザ監

査レコードを、終了前に（終了点2278）予算監査追跡UDEにセーブする（ブロック2274、2276）。

図42bを見て、最初の6個のステップ（ブロック2280～2290）が、何らかのユーザ行動（例えば新しい情報にアクセスすることを求める要求、新しい予算の要求など）に応答してユーザVDEノードによって行われ得る。BUDGETメソッド2250のこの「管理的要求」呼び出しは、監査追跡を用意し得る（ブロック2280、2282）。メソッドは次に、適切な予算の管理的処理の要求を、要求キューに入れ得る（ブロック2284、2286）。最後に、メソッドは、適切な監査追跡情報をセーブし得る（ブロック2288、2290）。しばらくたった後、ユーザVDEノードは、通信監査追跡を用意し得（ブロック2292、2294）、次に予算管理的要求を管理的オブジェクトに書き込み得る（ブロック2296）。このステップは、例えば、予算UDE、予算監査追跡UDE（単数または複数）、および予算管理的要求レコード（単数または複数）などのソースから必要になるような情報を、安全データベースから入手し得る（ブロック2298）。

ブロック2296は次に、管理的オブジェクトをVDE金融プロバイダに通信するか、または、ブロック2296は、管理的オブジェクトをそのような通信が起こるように取り決めを行う別の通信プロセスまたはメソッドに渡してもよい。所望であれば、メソッド2250は次に、終了前に（終了点2304）通信監査追跡（ブロック2230、2302）をセーブし得る。

図42cは、「管理的応答」モードで動作する、好適な実施態様で提供される例のBUDGETメソッド2250によって行われるプロセス制御ステップの一例を示す、フローチャートである。図42cに示すステップは、例えば、図42b（ブロック2296）によって作成された（そして例えばVDE管理者に通信された）予算管理的要求を含む、管理的オブジェクトを受信した、VDE金融プロバイダによって行われる。

管理的オブジェクトを受信すると、BUDGETメソッド2250は、VDE金融プロバイダサイトにおいて、予算通信および応答監査追跡を用意し得（ブロック2306、2308）、次に管理的オブジェクトをアンパック(unpack)して、その中に含まれる予

算要求（単数または複数）、監査追跡（単数または複数）、およびレコード（単数または複数）を取り出す（retrieve）（ブロック2310）。管理的オブジェクトから取り出されたこの情報は、VDE金融プロバイダによって、その安全データベース内に書き込まれる（ブロック2312）。VDE金融プロバイダは次に、予算要求（単数または複数）を取り出して、要求を処理するために実行することが必要な応答メソッドを決定する（ブロック2314、2316）。BUDGETメソッド2250は、要求レコード（単数または複数）に含まれるイベント（単数または複数）を、適切な応答メソッドに送り得、RESPONSEメソッドに基づいて応答レコードおよび応答要求を生成し得る（ブロック2318）。ブロック2318で行われるプロセスは、適切な新しい応答レコードをVDE金融プロバイダの安全データベースに書き込むことによって、予算要求を満足し得る（ブロック2320）。BUDGETメソッド2250は次に、これらの予算管理的応答レコードを管理的オブジェクト中に書き込み（ブロック2322、2324）、これを次に、予算要求を開始したユーザノードに通信し戻し得る。BUDGETメソッド2250は次に、通信および応答処理監査追跡情報を、終了前に（終了点2330）適切な監査追跡UDE（単数または複数）にセーブし得る（ブロック2326、2328）。

図４２ｄは、「管理的返答」モードで動作する、代表例のBUDGETメソッド2250によって行われるプログラム制御ステップの一例を示す、フローチャートである。図４２ｄに示すステップは、例えば、予算関連情報を含む管理的オブジェクトを受信した、VDEユーザノードによって行われ得る。BUDGETメソッド2250はまず、予算管理的および通信監査追跡を用意し得る（ブロック2332、2334）。次にBUDGETメソッド2250は、レコードおよび要求を受信した管理的オブジェクトから抽出し、返答レコードをVDE安全データベースに書き込む（ブロック2336、2338）。VDEユーザノードは次に、予算管理的および通信監査追跡情報を、適切な監査追跡UDE（単数または複数）（ブロック2340、2341）にセーブする。

しばらくたった後に、ユーザVDEノードは、返答レコードを安全データベースから取り出して、その処理のためにどのメソッドが必要であるかを決定し得る（ブロック2344、2346）。VDEユーザノードは、オプションとして、返答イベン

トの処理結果を記録するために通信監査追跡を用意し得る（ブロック2342、2343）。BUDGETメソッド2250は次に返答レコード（単数または複数）に含まれるイベント（単数または複数）をREPLYメソッドに送り得、安全データベースレコードを、新しい予算レコードを挿入する、古い予算レコードを削除するおよび／または予算レコードに変化を適用するなど必要に応じて生成／更新する（ブロック2348、2350）。BUDGETメソッド2250は次に、監査追跡を（必要であれば）書き込む（ブロック2354、2355）終了（終了点2356）前に、返答レコードを安全データベースから削除し得る（ブロック2352、2353）。

Ｂ．登録

図43a～図43dは、好ましい実施の形態により提供されるREGISTER（登録）メソッド2400の代表例によりおこなわれるプログラム制御ステップの一例を示すフローチャートである。この例では、REGISTERメソッド2400は、「使用」モードで動作する時には図43aに示されているステップ例をおこない、「管理リクエスト」モードで動作する時には図43bに示されているステップ例をおこない、「管理応答」モードで動作する時には図43cに示されているステップをおこない、「管理返答」モードで動作する時には図43dに示されているステップをおこなう。

図43aに示されているステップは、例えば、何らかのアクションに応答して、ユーザによって、またはユーザのために、ユーザVDEノードでおこなわれうる。例えば、ユーザは、自分自身に対してまだ（つまり、今でも）正しく登録されていないオブジェクトへのアクセスを要請できる。このようなユーザリクエストに応答して、REGISTERメソッド2400は、リクエストされているオブジェクトが既に登録されたかどうかを判定する（判定ブロック2406）前に、登録監査追跡UDE（ブロック2402、2404）を予めおこなうことができる。もし、オブジェクトが既に登録されているのなら（判定ブロック2406に対する「イエス」エグジット）、REGISTERメソッドは、（終端点2408で）終了することができる。もし、オブジェクトがまだ登録されていないのなら（判定ブロック2406に対する「ノー」エグジット）、REGSITERメソッド2400は、VDEノードの安全データベースPERC 808および／または登録MDE（ブロック2410）にアクセスすることができる。REGISTERメソッド2

400は、このPERC 808および／または登録MDEから適当な登録記録セットを抽出することができ(ブロック2412)、かつそのオブジェクトを登録するのに必要とされる、要求されたエレメントのすべてが存在しているかどうかを判定することができる(判定ブロック2414)。もし(少なくとも１つの)何らかの部分が欠けているのなら(判定ブロック2414に対する「ノー」エグジット)、REGISTERメソッド2400は、登録リクエストが通信マネージャへと記録されるのをキューイングし、その後、キュ

ーイングされたリクエストが満たされるまでREGISTERメソッドをサスペンドすることができる(ブロック2416、2418)。ブロック2416は、例えば、登録リクエストをVDE配付者へと通信する効果を有しうる。そのリクエストが満たされ、登録リクエスト記録が受け取られる(ブロック2420)と、判定ブロック2414のテストが満たされ(判定ブロック2414に対する「イエス」エグジット)、REGISTERメソッド2400は進むことができる。この段階で、REGISTERメソッド2400は、ブロック2410でアクセスされたPERC 808により許可されたメソッドオプションセットの中から登録オプションをユーザが選択できるようにする(ブロック2422)。１つ簡単な例を挙げれば、PERC 808は、ユーザに対して、VISAまたはマスターカードによる支払いは許可するが、アメリカンエクスプレスによる支払いは許可しない。ブロック2422は、ユーザに対して、そのVISAカードを使って支払うのか、あるいはそのマスターカードを使って支払うのか選択するように要請するプロンプトを表示することができる(ブロック2424)。REGISTERメソッド2400は、好ましくは、ユーザの選択した登録オプションの有効性を検査し、もし初期ユーザオプションが無効であるのなら、ユーザに対して別のオプションを選択するようにリクエストする(ブロック2426、判定ブロック2428に対する「ノー」エグジット)。いったんユーザが、要求された登録オプションの選択をすべて完了し、それらの選択すべての有効性が認められれば(判定ブロック2428に対する「イエス」エグジット)、REGISTERメソッド2400は、このオブジェクトおよびこのユーザに対応し、このユーザによりなされたユーザ登録選択を具体的に表すユーザ登録テーブル(URT)を、PERC 808および／または登録MDEにより要求されるその他の登録情報と共に書き込

むことができる（ブロック2430、2432）。その後、REGISTERメソッド2400は、（終端点2436で）終了する前に、登録監査記録を安全データベースへと書き込むことができる（ブロック2432、2434）。

図43bは、REGISTERメソッド2400の「管理リクエスト」モードの一例を示している。この管理リクエストモードは、VDE配付者へと、または登録情報をリクエストしているその他の適切なVDE加入者へと通信するための、適切な

管理オブジェクトを発生するために、VDEユーザシステム上でおこなわれうる。よって、例えば、図43bに示されているステップは、図43aに示されている「登録リクエストの記録をキューイングする」ブロック2416の一部としてもおこなわれうる。登録管理リクエストをおこなうために、REGISTERメソッド2400は、まず通信監査追跡を予めおこない（ブロック2440、2442）、その後、安全データベースにアクセスして登録に関するデータを得ることができる（ブロック2444）。このように安全データベースへとアクセスすることにより、例えば、登録されているオブジェクトの保有者および／または出版者が、人口統計、ユーザ自身、またはそのユーザに関するその他の情報を見出すことが可能になる。具体的な例として、現在、登録されているオブジェクトがスプレッドシートソフトウェアプログラムである場合を考える。そのオブジェクトの配付者は、そのユーザが登録した他のソフトウェアは何であるかを知りたいと思うことがある。例えば、配付者は、もし、その同じ配付者により配付されている多数のソフトウェア製品の「組み物」をユーザが登録するのなら、進んで優先的な価格を提示しようとするかもしれない。よって、標準的なソフトウェアパッケージの大半で中に入れてある「ユーザ登録」カードにより懇請されている情報の種類は、好ましい実施の形態では、登録時に懇請され、自動的に得られるようにすることができる。ユーザのプライバシー権を保護するために、REGISTERメソッド2400は、このようなユーザ固有のデータをプライバシーフィルタに通すことができる（ブロック2446）。このフィルタは、ある種の情報が外界に顕示されることをユーザが防止できるように、少なくとも部分的にはユーザによりカスタマイズされうる。REGISTERメソッド2400は、結果として得られた情報を、オブジェクトおよびその他の適切なパラメータを識別

する適切な登録リクエスト情報とともに管理オブジェクトへと書き込むことができる（ブロック2248、2450）。REGISTERメソッド2400は、その後、この管理オブジェクトを通信操作者にわたすことができる。REGISTERメソッド2400は、その後、（終端点2456で）終了する前に、通信監査追跡を保存することができる（ブロック2452、2454）。

図43cは、図43bのブロック2448により送られた登録管理オブジェクトを受け取ると、直ちにVDE配付者によりおこなわれうるREGISTERメソッド2400のステップを含んでいる。REGISTERメソッド2400は、この「管理応答」モードでは、まず適切な監査追跡を予めおこない（ブロック2460、2462）、その後、受け取った管理オブジェクトの包みを開いて、関連する（１つ以上の）登録リクエストのコンフィギュレーション情報を安全データベースへと書き込むことができる（ブロック2464、2466）。REGISTERメソッド2400は、その後、安全データベースから管理リクエストを取り出し、リクエストを処理するためには、どの応答メソッドをランさせればよいかを決定する（ブロック2468、2470）。もし、ユーザがそのオブジェクトを登録するのに十分な情報を提供しなければ、REGISTERメソッド2400は、失敗することがある（ブロック2472、2474）。そうでなければ、REGISTERメソッド2400は、適切な（１つ以上の）リクエスト記録に含まれている（１つ以上の）イベントを適切な応答メソッドに送り、応答記録および応答リクエスト（例えば、（１つ以上の）PERCおよび／またはUDE）を発生して、それらを安全データベースへと書き込むことができる（ブロック2476、2478）。その後、REGISTERメソッド2400は、適切な登録管理応答記録を管理オブジェクトへと書き込むことができる（ブロック2480、2482）。このような情報としては、例えば、１つ以上の置き換えPERC 808、メソッド、（１つ以上の）UDEなどがある（ブロック2482）。これにより、例えば、配付者が、オブジェクトを登録するのに十分な情報のみをユーザに与える限定権利パーミッションを配付し、その後、登録されると直ちに、その限定権利パーミッションをより広いパーミッション範囲に置き換えることによって、ユーザに対して、それらのオブジェクトへのより完全なアクセスを承認することができる。REGISTERメソッド2400は、その後、（終端点2488で）終了する前に

、通信および応答処理監査追跡を保存することができる（ブロック2484、2486）。

図43dは、図43cのブロック2480により発生／伝送された管理オブジェクトを受け取ると直ちにVDEユーザノードによりおこなわれうるステップを示している。図43dに示されているステップは、BUDGETメソッドの管理返答処理のための、図42dに示されているステップに非常によく似ている。

Ｃ．監査

図44a～図44cは、好ましい実施の形態により提供されるAUDIT（監査）メソッド2520の代表例によりおこなわれるプログラム制御ステップのいくつかの例を示すフローチャートである。上述した例と同様に、AUDITメソッド2520は、好ましい実施形態例では、３つの異なる動作モードを提供する。図44aは、「管理リクエスト」モードでAUDITメソッドによりおこなわれる各種ステップを示しており、図44bは、「管理応答」モードでこのメソッドによりおこなわれる各種ステップを示しており、図44cは、「管理返答」モードでこのメソッドによりおこなわれる各種ステップを示している。

図44aに示されているように「管理リクエスト」モードで動作するAUDITメソッド2520は、典型的には、ユーザによる、またはユーザのためのあるリクエストに基づいて、例えばVDEユーザノードにおいておこなわれる。例えば、ユーザは、監査をリクエストしたかもしれないし、VDE内容プロバイダまたはその他のVDE加入者への監査情報の通信を開始するタイマーが時間切れになったかもしれない。好ましい実施の形態では、同一の処理全体についてそれぞれ異なる監査が、それぞれ異なるVDE加入者によりおこなわれてもよい。ある特定の「監査」メソッド2520の実施（invocation）は、関係するVDE加入者のいずれか一人（または全員）に対して開始されうる。AUDITメソッド2520を実施すると直ちに、このメソッドは、管理監査追跡の監査を予めおこなうことができる（よって、好ましい実施の形態では、監査処理そのものが監査されうる）（ブロック2522、2524）。その後、AUDITメソッド2520は、管理処理リクエストをキューイングし（ブロック2526、2528）、そして、管理監査追跡の監査を安全データベースに保存することができる（ブロック2530、2532）。しばらくたった後で、AUDITメソッド2520は、通信監査追

跡を予めおこない（ブロック2534、2536）、その後、（１つ以上の）監査管理リクエストを、具体的なUDE、（１つ以上の）監査追跡UDEおよび／または安全データベースに格納されている（１つ以上の）管理記録に基づいて、１つ以上の管理オブジェクトへと書き込

むことができる（ブロック2538、2540）。AUDITメソッド2520は、その後、（終端点2546で）終了する前に、適切な情報を通信監査追跡に保存することができる（ブロック2542、2544）。

図44bは、図44aのブロック2538により発生され、通信された管理オブジェクトを受け取ると直ちに、VDE内容プロバイダ、財務プロバイダあるいはその他の監査VDEノードによりおこなわれるステップの例を示している。この「管理応答」モードでのAUDITメソッド2520は、まず、通信および応答監査追跡の監査を予めおこない（ブロック2550、2552）、その後、受け取った管理オブジェクトの包みを開き、そこに含まれている（１つ以上の）監査リクエスト、（１つ以上の）監査追跡および（１つ以上の）監査記録を取り出して、それらを安全（secured）データベースへと格納することができる（ブロック2554、2556）。その後、AUDITメソッド2520は、それら（１つ以上の）監査リクエストを安全データベースから取り出し、そのリクエストを処理するためにランすべき応答メソッドを決めることができる（ブロック2558、2560）。この段階で、AUDITメソッド2520は、（１つ以上の）リクエスト記録に含まれている（１つ以上の）イベントを適切な応答メソッドに送り、このメソッドに基づいて、（１つ以上の）応答記録およびリクエストを発生することができる（ブロック2562、2564）。処理ブロック2562は、外界への通信を含んでいてもよい。

例えば、AUDITメソッド2520は、この時点で、例えばユーザの銀行口座またはその他の銀行口座に対する電子財産転送をおこなうために、外部の処理をコールしてもよい。AUDIT管理応答は、もし望みとあれば、VDEを既存の１つ以上のコンピュータシステムにインタフェースする外部処理をコールすることもできる。この外部処理には、ユーザの口座番号、PIN、残高のドル、あるいは、現在処理されているVDE監査追跡で設定されている、またはそれに関連づけられたその他何

らかの情報を通すことができる。この外部処理は、非VDEのホストと通信することができ、それに通された情報をこれらの通信の一部として用いることができる。例えば、外部処理は、銀行へと提出するファイルの中に自動化された手形交換所（ACH）記録を発生することができる。このメカニズムは、どの

ような財務団体における銀行口座でも自動的に貸し方あるいは借り方に記入する能力を提供できる。この同じメカニズムは、請求口座に対してVDEベースの請求金額を提出することによって、既存のクレジットカード（例えば、VISA）ネットワークと通信するのに用いられうる。

いったん（１つ以上の）適切な監査応答記録が発生されると、AUDITメソッド2520は、（１つ以上の）監査管理記録を管理オブジェクトへと書き込み、その監査リクエストを発生したVDEユーザノードに通信し返すことができる（ブロック2566、2568）。その後、AUDITメソッド2520は、（終端点2574で）終了する前に、通信および応答処理監査情報を（１つ以上の）適切な監査追跡に保存することができる（ブロック2570、2572）。

図44cは、図44bのブロック2566により発生され、送られた管理オブジェクトを受け取ると直ちに、VDEユーザノードにおいて再びAUDITメソッド2520によりおこなわれうるステップの一例を示している。図44cに示されているステップ2580～2599は、「管理返答」モードにおけるREGISTERメソッド2400のための、図43dに示されているステップに似ている。簡単にいうと、これらのステップは、管理オブジェクトから適切な応答記録を受け取り、抽出すること（ブロック2584）と、その後、受け取った情報を適切に処理することによって、安全データベースの記録を更新し、その他の必要なアクションをおこなうこと（ブロック2595、2596）とを伴う。

イベントによりドライブされた、内容ベースのメソッドの例

VDEメソッド1000は、安全処理に対して非常にフレキシブルで、きわめてモジュール性の高いアプローチを提供するように設計される。「ユーザイベント」にサービスするための完全なVDE処理は、典型的には、いくつかのメソッド1000の組み合わせとして構成されうる。一例を挙げれば、オブジェクト300から内容あ

るいはその他の情報を読み出すための典型的な処理は、以下のメソッドを伴うことがある。

・ EVENTメソッド

・ METERメソッド

・ BILLINGメソッド

・ BUDGETメソッド

図45は、あるイベントに応答して、VDE 100により順次おこなわれる一連のメソッドの一例である。この例では、あるイベントが発生すると、EVENTメソッド402は、そのイベントの「重要性を判定する」ことによって、それが有意であるかどうかを判定する。すべてのイベントが有意であるわけではない。例えば、もし制御処理におけるEVENTメソッド1000が、使用法は、読まれたページの数に基づいて計量処理される（metered）べきであることを命ずるのなら、１ページ未満の情報を読みたいというユーザリクエスト「イベント」は、無視されることがある。別の例では、もしシステムイベントが、いくつかの数のバイトを読みたいというリクエストを表し、かつEVENTメソッド1000が、パラグラフを計量処理するように設計された制御処理の一部であるのなら、このEVENTメソッドは、読み出しリクエストを評価することによって、リクエストされたバイトには、いくつのパラグラフが表現されているかを決めることができる。この処理は、以下にさらに詳細に説明する「原子エレメント」へのマッピングを伴うことがある。

EVENTメソッド402は、関連する具体的な制御メソッドには有意ではないイベントをフィルタリングして除く。EVENTメソッド402は、重要性の判定されたイベントをMETER処理1404に渡すことができる。この処理は、それ固有の特定の基準に基づいて、イベントを計量処理するか、または破棄する。

加えて、この好ましい実施の形態は、「プリチェック」と呼ばれる最適化を実現する。EVENTメソッド／処理402は、計量処理、課金および予算に関する情報に基づきこの「プリチェック」をおこなうことによって、あるイベントに基づく処理が許可されるかどうかを判定する。例えば、ユーザが、ある情報の内容にアクセスする時、その予算を既に超えている結果、それ以上のアクセスが許可されな

い場合を考える。BUDGETメソッド408はこのような判定を下すことができるとはいうものの、BUDGETメソッド404および／またはBILLINGメソッド

406によりおこなわれる記録および処理は、例えば、実際には拒絶されたアクセスについてユーザが請求を受けることを防止するために、「やりなおし」しなければならないこともある。また、「やりなおし」しなければならない取引の数を少なくするために、EVENTメソッド402内で「プリチェック」をおこなうほうが、効率がいいこともある。

METERメソッド404は、監査記録を例えば、計量「追跡」UDE 1200に格納し、そのイベントに関する情報も計量UDE 1200に格納することができる。例えば、METERメソッド404は、内容がアクセスされる度に、計量UDE 1200内の「計量」値をインクリメントまたはデクリメントすることができる。これら２つの異なるデータ構造（計量UDEおよび計量追跡UDE）は、例えば、内部操作を目的としてつけられている記録とは別に保守される、リポートを目的とした記録をつけることを許可するように保守されうる。

いったん、イベントがMETERメソッド404により計量処理されると、計量処理されたそのイベントは、BILLINGメソッド406により処理されうる。BILLINGメソッド406は、どのぐらいの予算がそのイベントにより消費されるかを決め、計量と予算との間の調停に役立つ記録をつける。よって、例えば、BILLINGメソッド406は、予算UDEから予算情報を読み出し、課金情報を課金UDEに記録し、１つ以上の監査記録を課金追跡UDEに書き込むことができる。ある課金追跡の情報が計量および／または予算追跡の情報を複製することはあるものの、その課金追跡の情報は、例えば、内容の作成者102が、一定額の支払いを期待できるようにするのに役立ち、また、作成者102に送られた計量追跡の情報を、例えば独立採算プロバイダへと送られた予算追跡の情報と調停する調停チェックとしてもはたらく。

その後、BILLINGメソッド406は、その後、イベントをBUDGETメソッド408に渡すことができる。BUDGETメソッド408は、限界を設定し、その限界に関連づけられた取引の情報を記録する。例えば、BUDGETメソッド408は、予算情報を予算UDEに格納し、監査記録を予算追跡UDEに格納することができる。BUDGETメソッド408

は、結果的には、BILLINGメソッド406により指

定される量だけデクリメントされる予算UDEにおける「予算残高」フィールドになることがある。

いったん各種メソッド402、404、406および408がそのイベントを処理し終わったら、その情報の内容が明らかにされてもよいし、またはその他のアクションが起こされてもよい。

前述したように、好ましい実施の形態におけるPERC 808には、制御処理におけるその他の要求されたメソッドのパフォーマンスを実際に監督する、「制御メソッド」が提供されてもよい。図46は、図45の要求されたメソッド／処理402、404、406および408が、制御メソッド410によりどのように組織され、制御されうるかを示している。制御メソッド410は、イベントをコールして迅速に処理するか、さもなくば他のすべてのメソッド402、404、406および408を実施するか、さもなくば、ある「イベント」に応答しておこなわれる処理を監督する。

制御メソッドは、PERC 808内の制御セット906のレベルではたらく。これらのメソッドは、獲得された異種のメソッド1000間の構造、論理および制御の流れを提供する。このメカニズムにより、内容プロバイダが、望みのどのような処理の連鎖でも生成することが可能になり、また、その具体的な処理の連鎖を、下流側の再配付者たちが（許容された限界内で）改変することも可能になる。このような制御メソッドの概念により、大きな柔軟性が実現する。

図47は、METERメソッド404、BUDGETメソッド406およびBILLINGメソッド408を「集合」処理フローの中に集結する「集合」メソッド412の一例を示している。集合メソッド412は、例えば、計量処理、予算作成および課金のさまざまな要素を単一のメソッド1000の中に組み合わせることができる。集合メソッド412は、METERメソッド404、BUDGETメソッド406およびBILLINGメソッド408を一括処理する結果として効率の向上を実現可能とするが、モジュール性が低下するので柔軟性を低下させてしまう。

多数の異なるメソッドを、同時に実施することができる。図48は、多数のMETERメソッド404および多数のBUDGETメソッド1408を用いる、好まし

い実施の形態によるイベント処理の一例を示している。いくつかのイベントを、独立して、または累積するように作用する異なる多数の要求されたメソッドにかけることができる。例えば、図48に示されている例では、計量メソッド404aは、METERメソッド404bにより保守されている計量追跡および計量情報記録からは独立した計量追跡および計量情報記録を保守することができる。同様に、BUDGETメソッド408aは、BUDGETメソッド408bにより保守されている記録からは独立して、記録を保守することができる。いくつかのイベントは、BILLINGメソッド408をバイパスとしながら、それでも計量メソッド404aおよびBUDGETメソッド408aにより処理されうる。それぞれ異なる変形からなる多種多様な組み合わせが可能である。

ＶＤＥメソッドの代表例

メソッド1000には、実質的に無限の組み合わせがあり、またそのうちのいくつかはユーザにより規定されうるものもあるが、好ましい実施の形態では、VDE 100により提供されるより基本的なオブジェクト操作およびその他の機能の大半を制御するために、いくつかの基本的な「使用」型のメソッドが好ましくは用いられる。例えば、典型的には、以下の高レベルメソッドが、オブジェクト操作用に提供されることになる。

- OPENメソッド
- READメソッド
- WRITEメソッド
- CLOSEメソッド

OPENメソッドは、ある入れ物の内容にアクセスできるように、その入れ物を開くことを制御するのに用いられる。READメソッドは、ある入れ物の内容へのアクセスを制御するのに用いられる。WRITEメソッドは、ある入れ物への内容の挿入を制御するのに用いられる。CLOSEメソッドは、開かれていたある入れ物を閉じるのに用いられる。

OPEN、READ、WRITEおよび／またはCLOSE法により要求されるステップのうちのいくつかをおこなうために、補助的なメソッドがいくつか提供される。

このような補助的メソッドには、以下のものがある。

- ACCESSメソッド
- PANICメソッド
- ERRORメソッド
- DECRYPTメソッド
- ENCRYPTメソッド
- 内容DESTROYメソッド
- INFORMATIONメソッド
- OBSCUREメソッド
- FINGERPRINTメソッド
- EVENTメソッド
- CONTENTメソッド
- EXTRACTメソッド
- EMBEDメソッド
- METERメソッド
- BUDGETメソッド
- REGISTERメソッド
- BILLINGメソッド
- AUDITメソッド

ACCESSメソッドは、開かれた入れ物に関連づけられた内容（その内容は、どこにあってもよい）に物理的にアクセスするのに用いられうる。PANICメソッドは、もし安全性の侵害が検出されれば、VDEノードの少なくとも一部をディセーブルするのに用いられうる。ERRORメソッドは、エラー状況を操作するのに用いられうる。DECRYPTメソッドは、暗号化された情報を復号化するのに用いられる。ENCRYPTメソッドは、情報を暗号化するのに用いられる。内容DESTROYメソッドは、入れ物の中の具体的な内容にアクセスする能力を破壊するのに用いられる。INFORMATIONメソッドは、入れ物の内容に関する公開

情報を提供するのに用いられる。OBSCUREメソッドは、開かれた入れ物から読み

出された内容の価値を減ずる（例えば、表示されている画像の上に単語「SAMPLE」を書き込む）のに用いられる。FINGERPRINTメソッドは、内容にマークをつけることによって、誰がその内容を安全な入れ物から明らかにしたかを示すために用いられる。イベントメソッドは、他のメソッドによる応答のために、イベントを異なるイベントに変換するのに用いられる。

オープン

図49は、OPENメソッド1500の一例について好ましい実施の形態による処理制御ステップの一例を示すフローチャートである。異なるOPENメソッドでは、詳細なステップもそれぞれ異なってくる。しかし、図49に示されているOPENメソッドは、好ましい実施の形態により提供される比較的、多くの特徴を備えた「オープン」メソッドの代表例である。図49は、OPENメソッドの巨視的な図を示している。図49a～図49fは、全部合わせると、図49に示されているメソッドを実施するためにおこなわれる詳細なプログラム制御されたステップの一例を示している。

OPENメソッドの処理は、「オープンイベント」からスタートする。このオープンイベントは、ユーザアプリケーションによって、または制御を獲得するか、それに割り込む、オペレーティングシステムの割り込みあるいはその他さまざまなメカニズムによって発生される。例えば、ユーザアプリケーションは、VDEの入れ物の中に格納されている特定の内容物にアクセスするリクエストを発することができる。別の例としては、別のメソッドが、コマンドを発することもある。

図示されている例では、オープンイベントは、制御メソッド1502により処理される。制御メソッド1502は、他のメソッドにそのイベントの処理をコールすることもできる。例えば、制御メソッド1502は、EVENTメソッド1504、METERメソッド1506、BILLINGメソッド1508およびBUDGETメソッド1510をコールすることもできる。必ずしもOPEN制御メソッドのすべてが、このような追加のメソッドをコールするわけではなく、図49に示されている

OPENメソッド1500は、代表例にすぎない。

制御メソッド1502は、オープンイベントの記述をEVENTメソッド1504に渡す。EVENTメソッド1504は、例えば、オープンイベントにパーミッションが与えられて

いるかどうかを判定し、そのオープンイベントが、METERメソッド1506、BILLINGメソッド1508および／またはBUDGETメソッド1510により処理される必要があるという意味合いで有意であるかどうかを判定する。EVENTメソッド1504は、監査追跡UDE内で監査追跡情報を保守し、イベントメソッドデータエレメント（MDE）を用いることによって、イベントのパーミッションおよび有意性を判定することができる。EVENTメソッド1504はまた、オープンイベントを「原子エレメント」へとマッピングし、METERメソッド1506、BILLINGメソッド1508および／またはBUDGETメソッド1510により処理されうるカウントの中にマッピングすることもできる。

OPENメソッド1500では、いったんEVENTメソッド1504がコールされ、そのリターンに成功すると、制御メソッド1502は、次にMETERメソッド1506をコールし、そのMETERメソッドに原子エレメントおよびEVENTメソッド1504によりリターンされたカウントを渡すことができる。METERメソッド1506は、監査追跡情報をMETERメソッドの監査追跡UDEの中で保守し、計量情報をMETERメソッドのUDEの中で保守することができる。好ましい実施の形態では、METERメソッド1506は、完了に成功したとすると、計量値を制御メソッド1502にリターンする。

好ましい実施の形態では、制御メソッド1502は、METERメソッド1506が完了に成功したという通知を受け取ると直ちに、BILLINGメソッド1508をコールする。制御メソッド1502は、METERメソッド1506により提供された計量値をBILLINGメソッド1508に渡すことができる。BILLINGメソッド1508は、BILLINGメソッドのマップMDEにおいて保守されている課金情報を読み出して更新し、監査追跡をBILLINGメソッドの監査追跡UDEにおいて保守し更新することができる。BILLINGメソッド1508は、課金額と完了コードとを制御メソッド1502にリターンすることができる。

BILLINGメソッド1508が完了に成功したとすると、制御メソッド1502は、BILLINGメソッド1508により提供された課金価格をBUDGETメソッド1510に渡すことができる。BUDGETメソッド1510は、BUDGETメソッドのUDE内の予算情報を読み出して更新し、BUDGETメソッドの監査追跡UDE内の監査追跡情報を保守することができ

る。BUDGETメソッド1510は、予算金額を制御メソッド1502にリターンし、（このタイプのイベントの場合）オープンイベントがユーザの予算を超えたかどうかを示す完了コードをリターンすることができる。

BUDGETメソッド1510が完了すると、制御メソッド1502は、チャネルを生成し、後でおこなわれるREADメソッドへのコールに備えて、読み出し／使用制御情報を確定することができる。

図49a～図49fは、図49に示されているOPENメソッド1500の例のより詳細な記述である。図49aを参照すると、オープンイベントに応答して、制御メソッド1502は、まず開かれるべきオブジェクトの識別子と、開かれるべきオブジェクトをリクエストしたユーザの識別子とを判定する（ブロック1520）。次に、制御メソッド1502は、開かれるべきオブジェクトが、このユーザに登録されているかどうかを判定する（判定ブロック1522）。好ましい実施の形態では、この判定は、少なくとも部分的には、ブロック1520により判定された特定のオブジェクトおよび特定のユーザに関連づけられたPERC 808およびユーザ権利テーブル（URT）エレメントを読み出すことによっておこなわれる（ブロック1524）。もしユーザがこの特定のオブジェクトについて登録されていないのなら（判定ブロック1522に対する「ノー」エグジット）、制御メソッド1502は、そのオブジェクトについてREGISTERメソッドをコールし、いったん登録が完了すれば、OPENメソッド1500を再開することができる（ブロック1526）。REGISTERメソッドのブロック1526は、独立した処理でありうるし、時間非依存でもありうる。例えば、REGISTERメソッドを完了するのに比較的長い時間を要することがある（例えば、VDE配付者や、登録を提供する責任をもつその他の加入者が、この特定のオブジェクトについてユーザを登録する前に、その

ユーザについてクレジットチェックをおこなうことを望む時など）。

このユーザおよびオブジェクトについて正しいURTが存在しており、そのオブジェクトはこのユーザについて登録されていることを示したとする（判定ブロック1522に対する「イエス」エグジット）と、制御メソッド1502は、そのオブジェクトが既にこのユーザに対して開かれているかどうか判定することができる（判

定ブロック1528)。このテストにより、既に開かれているオブジェクトを開くために冗長なチャネルを生成するのを避けることができる。そのオブジェクトがまだ開かれていないものとする（判定ブロック1528に対する「ノー」エグジット）と、制御メソッド1502は、チャネルを生成し、適切なオープン制御エレメントをそのチャネルに結びつける(ブロック1530)。このメソッドは、適切なオープン制御エレメントを安全データベース（または、例えば、移動するオブジェクトの場合には入れ物）から読み出し、このユーザに対してそのオブジェクトを開くことを制御するために、これら特定の適切な制御エレメントを「結びつける」か、「連結」する。よって、ブロック1530は、１つのイベントに、１つ以上の適切なメソッドコア、適切なロードモジュール、適切なユーザデータエレメント、および安全データベース（または入れ物）から読み出された適切なメソッドデータエレメントを関連づける(ブロック1532)。この時点で、制御メソッド1502は、（開始すべきOPENメソッドをスタートした）オープンイベントと、（ブロック1520により判定された）オブジェクトIDおよびユーザIDと、安全データベース「取引」(ブロック1536)を実現するための後続するEVENTメソッド1504、METERメソッド1506、BILLINGメソッド1508およびBUDGETメソッド1510に対する、ブロック1530により生成されたチャネルのチャネルIDとを指定する。そうする前に、制御メソッド1502は、監査処理を予めおこない(ブロック1533)、たとえ取引が失敗したり、干渉を受けたりしても、その取引の記録が存在しているように、監査情報を監査UDEへと書き込む(ブロック1534)。

EVENTメソッド1504によりおこなわれる詳細なステップは、図49bに述べられている。EVENTメソッド1504は、まず、もし必要なら、イベント監査追

跡を予めおこなう（ブロック1538）ことができる。これにより、EVENTメソッドの監査追跡UDEへと書き込む（ブロック1540）ことができる。EVENTメソッド1504は、次に、マップMDEを用いて、オープンイベントを原子エレメント番号およびカウントへとマッピングするステップ（ブロック1542）をおこなうことができる。EVENTメソッドのマップMDEは、安全データベースから読み出されうる(ブロック1544)。ブロック1542によりおこなわれるこのマッピング処理は、例えば、オ

ープンイベントが計量処理可能、課金可能あるいは予算作成可能であるかどうかを判定することができ、また、オープンイベントを、計量処理、課金および／または予算作成するための何らかの別個の原子エレメントに変換することができる。一例を挙げれば、ブロック1542は、オープンイベントと「オープン」原子エレメントとの間で１対１のマッピングをおこなうことができるし、そのオブジェクトが５回開かれるごとに１個のオープン原子エレメントを提供するにとどめることもできる。マップブロック1542は、好ましくは、オープンイベント、イベントカウント、原子エレメント番号、オブジェクトIDおよびユーザIDをリターンする。この情報は、EVENTメソッドの監査追跡UDE内に書き込まれうる（ブロック1546、1548）。好ましい実施の形態では、次に、EVENTメソッドが失敗したかどうかを判定するために、テスト（判定ブロック1550）がおこなわれる。具体的には、判定ブロック1550は、原子エレメント番号が発生されたかどうかを判定することができる。もし何の原子エレメント番号も発生されていなければ（これは、例えば、このオープンイベントが、METERメソッド1506、BILLINGメソッド1508および／またはBUDGETメソッド1510により処理するほど有意ではないことを意味する）、EVENTメソッド1504は、「失敗」完了コードを制御メソッド1502にリターンすることができる（判定ブロック1550に対する「ノー」エグジット）。

制御メソッド1502は、EVENTメソッド1504によりリターンされた完了コードをテストすることによって、それが失敗したのか、あるいは成功したのかを判定する（判定ブロック1552）。もし、EVENTメソッドが失敗したのなら（判定ブロック1552に対する「ノー」エグジット）、制御メソッド1502は、安全データベース取引を「ロールバックし」て（ブロック1554）、OPENメソッドが失敗したことを表示して自らをリターンする（ブロック1556）。この文脈において、安全データベース取引を「ロールバックする」とは、例えば、ブロック1540、1548により監査追跡UDEに施された変更を「元に戻す」ことを意味する。しかし、好ましい実施の形態においてブロック1554によりおこなわれるこの「ロールバック」は、ブロック1532、1534により制御メソッドの監査UDEに施された変更を「元に戻さない」。

EVENTメソッド1504が完了に成功したものとすると、制御メソッド1502は、次に、図49cに示されているMETERメソッド1506をコールする。好ましい実施の形態では、METERメソッド1506は、もし必要なら計量監査追跡を予めおこなう（ブロック1558）。このことは、典型的には、METERメソッドの監査追跡UDEへの書き込みを伴う（ブロック1560）。METERメソッド1506は、その後、METERメソッドのUDEを安全データベースから読み出し（ブロック1562）、計量UDEに含まれている計量値に適切なイベントカウントを加えることによって、計量UDEを修正し（ブロック1564）、その後、修正した計量UDEを安全データベースに再び書き込む（ブロック1562）。換言すれば、ブロック1564は、計量UDEを読み出し、それが含む計量カウントをインクリメントし、変更した計量UDEを安全データベースに再び書き込む。好ましい実施の形態では、METERメソッド1506は、その後、もし必要なら、METERメソッドの監査追跡UDEへと計量監査追跡情報を書き込むことができる（ブロック1566、1568）。METERメソッド1506は、好ましくは、次にテストをおこなうことによって、計量のインクリメントが成功したかどうかを判定する（判定ブロック1570）。METERメソッド1506は、完了コード（例えば、成功または失敗）およびブロック1564により決定された計量値を伴って制御メソッド1502にリターンする。

制御メソッド1502は、例えば、完了コードを調べることによって、METERメソッドが成功したかどうかをテストする（判定ブロック1572）。もしMETERメソッドが失敗したのなら（判定ブロック1572に対する「ノー」エグジット）、

制御メソッド1502は、安全データベース取引を「ロールバックし」（ブロック1574）、OPENメソッドが失敗したという表示を伴ってリターンする（ブロック1576）。METERメソッドが成功した（判定ブロック1572に対する「イエス」エグジット）ものとすると、制御メソッド1502は、BILLINGメソッド1508をコールし、このメソッドに、METERメソッド1506により提供された計量値を渡す。

BILLINGメソッド1508によりおこなわれるステップの一例は、図49dに述べられている。BILLINGメソッド1508は、もし必要なら、安全データベース内のBILLINGメソッドの監査追跡UDEへと書き込む（ブロック1580）ことによって、課金監査追跡を予めおこなうことができる（ブロック1578）。BILLINGメソッド1508は、そ

の後、安全データベースから読み出されたBILLINGメソッドのマップMDEを用いて、原子エレメント番号、カウントおよび計量値を課金額にマッピングすることができる（ブロック1582、1584）。例えば、価格リスト情報を含む、独立したBILLINGメソッドのマップMDEを提供することによって、この課金処理で、別々に配送可能な価格決定をおこなうことが可能になる。ブロック1582により発生される、結果として生じる課金額は、BILLINGメソッドの監査追跡UDEへと書き込まれ（ブロック1586、1588）てもよいし、制御メソッド1502へとリターンされてもよい。加えて、BILLINGメソッド1508は、課金額が、ブロック1582により正しく選択されたかどうかを判定する（判定ブロック1590）ことができる。この例では、ブロック1590によりおこなわれるテストは、広くいうと、リターンされた課金額を単に調べること以上のことを要求する。なぜなら、課金額は、BILLINGメソッドのマップMDEにより指定される予想できないいくつかのメソッドで変更されうるからである。次に、制御は、制御メソッド1502にリターンする。このメソッドは、BILLINGメソッド1508により提供された完了コードをテストすることによって、BILLINGメソッドが成功したのか、あるいは失敗したのか判定する（ブロック1592）。もし、BILLINGメソッドが失敗した（判定ブロック1592に対する「ノー」エグジット）のなら、制御メソッド1502は、安全データベース取引を「ロールバックし」て（ブロック1594）、OPENメソッドが失敗したという表示をリターンする（ブロック1596）。判定ブロック1592によりおこなわれたテストが、BILLINGメソッドの成功を示す（判定ブロック1592に対する「イエス」エグジット）と、制御メソッド1502は、BUDGETメソッド1510をコールすることができる。

その他のBILLINGメソッドは、例えば、価格決定情報を確定するために、サイト、ユーザおよび／または使用法情報を用いることができる。例えば、オブジェクトの存在または不在に関する情報は、「掘り物」の購入、競合値引きなどを確定するのに用いられうる。使用法のレベルは、使用法のそれぞれ異なるレベルについて価格の分かれ目を確定するBILLINGメソッドへと分解されうる。BILLINGメソッドは、通貨を換金する特徴をもっているので、購入および／または価格決定

を多数の異なる通貨でおこなうことを可能にする。あるイベントにより消費される予算金額を決定するためには、BILLINGメソッドの中に取り入れることができる、その他多くの可能性が存在する。

BUDGETメソッド1510によりおこなわれる詳細な制御ステップの一例は、図49eに述べられている。BUDGETメソッド1510は、もし必要なら、予算追跡UDEへと書き込むことによって、予算監査追跡を予めおこなうことができる（ブロック1598、1600）。BUDGETメソッド1510は、次に、課金額を予算価格に加算することによって、課金操作をおこなうことができる（ブロック1602）。この操作は、例えば、BUDGETメソッドのUDEを安全データベースから読み出し、それを修正した後、それを安全データベースに再び書き込むことによっておこなわれうる（ブロック1604）。BUDGETメソッド1510は、その後、予算監査追跡情報をBUDGETメソッドの監査追跡UDEに書き込むことができる（ブロック1606、1608）。この例では、BUDGETメソッド1510は、最後に、ブロック1602により計算された予算価格が範囲外であるかどうかを判定する（判定ブロック1610）ことによって、ユーザが予算を使い果たしたかどうかを判定することができる。もしユーザが予算を使い果たしたのなら（判定ブロック1610に対する「イエス」エグジット）、BUDGETメソッド1510は、「失敗完了」コードを制御メソッド1502にリターンすることができる。BUDGETメソ

ッド1510は、その後、制御メソッド1502にリターンし、制御メソッド1502は、BUDGETメソッドの完了コードが成功したかどうかをテストする（判定ブロック1612）。もしBUDGETメソッドが失敗したのなら（判定ブロック1612に対する「ノー」エグジット）、制御メソッド1502は、安全データベース取引を「ロールバックし」て、OPENメソッドが失敗したという表示を伴って自らをリターンする（ブロック1614、1616）。制御メソッド1502が、BUDGETメソッドは成功したと判定したものとすると、この制御メソッドは、図49fに示されている追加のステップをおこなうことができる。例えば、制御メソッド1502は、もし必要なら、ブロック1532において予めおこなわれた監査UDEへと監査情報を書き込むことによって、オープン監査追跡を書き込むことができる（ブロック1618、1620）。制御メソッド1502は、

その後、チャネルを確定するためにオブジェクトとユーザとに関連づけられたユーザ権利テーブルおよびPERCを用いて（ブロック1624）、読み出しイベント処理（ブロック1622）を確定することができる。このチャネルは、望みとあればVDEノード600のユーザ間で共有されてもよいし、指定されたユーザのみによって用いられてもよい。

制御メソッド1502は、その後、好ましい実施の形態では、読み出しチャネルの確立が成功したかどうかをテストする（判定ブロック1626）。もし読み出しチャネルが、確立に成功していなかったのなら（判定ブロック1626に対する「ノー」エグジット）、制御メソッド1502は、安全（secured）データベース取引を「ロールバックし」て、OPENメソッドが失敗したという表示を与える（ブロック1628、1630）。読み出しチャネルが確立に成功したものとすると（判定ブロック1626に対する「イエス」エグジット）、制御メソッド1502は、安全データベース取引を「委託する（commit）」ことができる（ブロック1632）。この安全データベース取引を「委託する」ステップは、好ましい実施の形態では、例えば、今おこなわれたばかりの安全取引に関連づけられた中間価格を削除し、かつ、ある例では、変更したUDEおよびMDEを安全データベースに書き込むことを伴う。いったん、安全な取引がブロック1632により委託されれば、それを「ロールバックする」ことは一般に不可能である。次に、制御メソッド1502は、終

了する（ブロック1636）前にオープン処理のためのチャネルを「解体」する（ブロック1634）ことができる。マルチタスクVDEノード環境のようなある種の構成では、オープンチャネルは、コンスタントに保守され、スタートするいかなるOPENメソッドによりいつでも用いられるようにしてもよい。その他の実現形態では、オープン処理のためのチャネルは、OPENメソッドがスタートするたびに、構成しなおされ、スタートしなおされてもよい。

読み出し

図50、図50a～図50fは、READメソッド1650の代表例をおこなうための処理制御ステップの例を示している。図50を図49と比較すれば、典型的には、OPENメソッド1500について説明したように、全体的には同様に高レベル処理が、READメソッ

ド1650についてもおこなわれることがわかる。よって、READメソッド1650が、ある読み出しイベントに応答して、制御メソッド1652をコールすると、制御メソッドは、これに応答して、EVENTメソッド1654、METERメソッド1656、BILLINGメソッド1658およびBUDGETメソッド1660を実施する。好ましい実施の形態では、READ制御メソッド1652は、復号化された内容を明らかにする前に、内容の指紋を採る、および／またはそれを曖昧にするためのメソッドをリクエストすることができる。

図50a～図50eは、図49a～図49eと同様である。もちろん、OPENメソッド1500およびREADメソッド1650の両方に同じユーザデータエレメントを用いることはできるものの、READメソッドのためのメソッドデータエレメントは全く違っていてもよい。加えて、ユーザデータエレメントは、読み出し用にオープン処理の場合とは対照的な、異なる監査、計量処理、課金および／または予算作成基準を設けてもよい。

図50fを参照すると、READ制御メソッド1652は、もし復号化された内容をユーザに明らかにしようとしているのなら、内容を復号化するのにどのキーを用いるべきかを決定しなければならない（ブロック1758）。READ制御メソッド1652は、部分的には、そのオブジェクト用のPERC 808に基づいて（ブロック1760）、このキー決定をおこなうことができる。READ制御メソッド1652は、次に、ACCESSメソッドをコールすることによって、復号化されるべき暗号化された内容を実際に得る（ブロック1762）。この内容は、ブロック1758により決定されたキーを用いて復号化される（ブロック1764）。READ制御メソッド1652は、次に「指紋」が望ましいかどうかを判定することができる（判定ブロック1766）。もしその内容の指紋採取が望まれるのなら（判定ブロック1766に対する「イエス」エグジット）、READ制御メソッド1652は、FINGERPRINTメソッドをコールすることができる（ブロック1768）。そうでなければ、READ制御メソッド1652は、復号化された内容を曖昧にするのが望ましいかどうかを判定する（判定ブロック1770）。もしそうなら、READ制御メソッド1652は、OBSCUREメソッドをコールしてこの機能を実行することができる（ブロック1772）。最後に、READ制御メソッド1652は、安全データ

ベース取引を委託し（ブロック1774）、望みとあれば読み出しチャネルを解体して（不図示）、終了することができる（ブロック1776）。

書き込み

図51、図51a～図51fは、好ましい実施の形態において、WRITEメソッド1780の代表例を実施するために用いられる処理制御ステップの例を示すフローチャートである。WRITEメソッド1780は、この例では、制御メソッド1782を用いて、EVENTメソッド1784、METERメソッド1786、BILLINGメソッド1788およびBUDGETメソッド1790をコールする。よって、好ましい実施の形態では、（既に入れ物に格納されている情報を上書きすることによって、またはその入れ物に情報を追加することによって）情報を入れ物に書き込むことは、入れ物を開いたり、入れ物から読み出したりすることが、計量処理され、課金され、かつ予算作成されるやり方と同様に、計量処理され、課金され、かつ予算作成されうる。図51に示されているように、WRITEメソッド1780の最終結果は、典型的には、内容を暗号化し、内容および関連する情報の入れ物テーブルを更新することによって新しい内容を反映させ、その内容をオブジェクトに書き込むこと

である。

WRITE制御メソッド1782のための図51aは、それぞれOPEN制御メソッドおよびREAD制御メソッドのための図49aおよび図50aに類似している。しかし、図51bは、オープンおよびリードの対応する図とはわずかに異なっている。具体的には、ブロック1820は、もしWRITE EVENTメソッド1784が失敗すれば、おこなわれる。このブロック1820は、EVENTメソッドのマップMDEを更新することによって、新しいデータを反映させる。このことは、ブロック1810により書き込まれた情報が、同じ（だが今や更新されている）EVENTメソッドのマップMDEに基づいて図51bのREADメソッドのブロック1678により読み出されるようにする必要がある。

図51fを見れば、いったんEVENT、METER、BILLINGおよびBUDGETメソッドが上首尾にWRITE制御メソッド1782にリターンすると、WRITE制御メソッドは、監査情報を監査UDEへと書き込んだ（ブロック1890、1892）後、内容が入れ物の中に書き込まれる前に、その内容を暗号化するのにどの鍵を用いるべきかを（そのオブジ

ェクトおよびユーザに対するPERCおよび選択可能な演算アルゴリズムに基づいて）決定する（ブロック1894、1896）。その後、CONTROLメソッド1782は、一例としてはENCRYPTメソッドをコールすることによって、内容を暗号化し（ブロック1898）、暗号化された内容をオブジェクトに書き込む（ブロック1900）。CONTROLメソッド1782は、その後、入れ物に対する内容（および関連する情報）を含むテーブルを更新することによって、新たに書き込まれた情報を反映させ（ブロック1902）、安全データベース取引（ブロック1904）を委託した後、リターンする（ブロック1906）。

クローズ

図52は、好ましい実施の形態において、CLOSEメソッド1920の代表例をおこなうための処理制御ステップの一例を示すフローチャートである。CLOSEメソッド1920は、開いているオブジェクトを閉じるのに用いられる。好ましい実施の形態では、CLOSEメソッド1920は、監査追跡を予めおこない、監査情報

を監査UDEに書き込む（ブロック1922、1924）。その後、CLOSEメソッド1920は、1以上の開いているオブジェクトをサポートする、および／または処理するために用いられている現在の（１つ以上の）チャネルを破壊することができる（ブロック1926）。上述したように、ある種の（例えば、マルチユーザあるいはマルチタスク）インストレーションでは、チャネルを破壊するステップは必要ない。なぜなら、チャネルは、同じユーザまたは異なるユーザに対して追加のオブジェクトを処理するために動作させたままにしておいてもよいからである。また、CLOSEメソッド1920は、この時点で、オブジェクトに関連づけられた適切な記録および資源を解放する（ブロック1926）。CLOSEメソッド1920は、その後、終了する前に、（もし必要なら）監査追跡を監査UDEへと書き込んでもよい（ブロック1928、1930）。

イベント

図53aは、好ましい実施の形態により提供されるEVENTメソッド1940のより一般的な例により設けられる処理制御ステップの例を示すフローチャートである。EVENTメソッドの例は、既に説明した図49b、図50bおよび図51bに述べられている。

図53aに示されているEVENTメソッド1940は、上述した例よりもいくらか一般化されている。上述したEVENTメソッドの例と同様に、EVENTメソッド1940も、イベントカウントおよびイベントパラメータと共に、イベントの識別子を受け取る。EVENTメソッド1940は、まず、適切な情報をEVENTメソッドの監査追跡UDEに書き込むことによって、（もし必要なら）EVENT監査追跡を予めおこなうことができる（ブロック1942、1944）。その後、EVENTメソッド1940は、安全データベースからEVENTメソッドのマップDTDを得て、ロードすることができる（ブロック1946、1948）。このEVENTメソッドのマップDTDは、この例では、引き続いて（ブロック1950、1952により）直ちに読み出され、アクセスされるEVENTメソッドのマップMDEのフォーマットを記述している。好ましい実施の形態では、MDEおよびUDEは、さまざまな異なるフォーマットのどれをもっていてもよく、それらのフォーマット

は、インストレーション、ユーザなどに依存してフレクシブルに指定されたり、動的に変更されてもよい。実際に、DTDは、EVENTメソッド1940に対して、EVENTメソッドのマップMDEからどのようにして読み出すかを記述する。DTDはまた、メソッドがどのようにしてMDEおよびDTDへと書き込むべきかを指定するのに用いられる。よって、DTDは、例えば、サードパーティに報告されるかもしれないデータ構造に、ある種の秘匿ユーザ情報が書き込まれるのを防止することによって、プライバシーフィルタを実施するのに用いられうる。

ブロック1950（「マップMDEを用いて、原子エレメント番号およびイベントカウントにイベントをマッピングする」）は、ある意味では、EVENTメソッド1940の「心臓」である。このステップは、イベントを、引き続いてコールされるメソッドが応答する対象である「原子エレメント番号」へと「マッピングする」。この「マッピング」ステップ1950の代表例といいうるものによりおこなわれる処理制御ステップの一例は、図53bに示されている。

図53bの例は、ある具体的な内容の断片からバイト範囲1001～1500をリクエストすることに関連づけられたREADイベントを、適切な原子エレメントに変換する処理を示している。この例によるEVENTメソッドのマッピング処理（図53aにおけるブロック1950）を、図53bに示されている代表的処理として詳しく述べること

ができる。

EVENTメソッドのマッピング処理1950は、まず、EVENTメソッドのマップDTD（1948）を用いてEVENTメソッドのMDE（1952）内のイベントコード（READ）を調べることによって、MDEの構造および内容を判定する。次に、イベントコードがMDEで見つかったかどうかを判定する（1956）ためにテストをおこなうことができる。もし見つからなければ（「ノー」分岐）、EVENTメソッドのマッピング処理は、イベントを原子エレメント番号およびカウントにマッピングすることなく、終了することがある（1958）。もしMDEにそのイベントが見つかったのなら（「イエス」分岐）、EVENTメソッドのマッピング処理は、その後、イベントの範囲（例えば、バイト1001～1500）を、MDEに格納されているイベント範囲マッピングテーブルに対する原子エレメントと比較する（ブ

ロック1960）。この比較の結果、１つ以上の原子エレメント番号が生じることもあるし、そのイベント範囲が、マッピングテーブルで見つからないこともある。次に、この比較の結果をテストする（ブロック1962）ことによって、何らかの原子エレメント番号がそのテーブルに見つかったかどうかを判定する。もし見つからなかったのなら（「ノー」分岐）、EVENTメソッドのマッピング処理は、原子エレメント番号あるいはカウントを１つも選択することなく、終了することがある（1964）。もし原子エレメント番号が見つかったのなら、この処理は、次に、イベント範囲から原子エレメントカウントを計算することができる（1966）。この例では、この処理は、上位バイト範囲を下位バイト範囲から減算する（例えば、1500－1001＋1＝500）ことによってリクエストされたバイト数を計算することができる。この例によるEVENTメソッドのマッピング処理は、その後、終了し（ブロック1968）、（１つ以上の）原子エレメント番号およびカウントをリターンすることができる。

その後、EVENTメソッド1940は、もし必要なら、EVENTの監査追跡をEVENTメソッドの監査追跡UDEへと書き込むことができる（ブロック1970、1972）。EVENTメソッド1940は、その後、（エグジットポイント1978で）原子エレメント番号およびイベントカウントを、コールしているCONTROLメソッド（あるいはその他の制御

処理）にわたす準備をすることができる。しかし、その前に、EVENTメソッド1940は、原子エレメントが選択されたかどうかをテストすることができる（判定ブロック1974）。もし選択された原子エレメントがなければ、EVENTメソッドは失敗することがある（ブロック1974）。このことは、いくつかの理由により起こりうる。例えば、EVENTメソッドは、もし、EVENTメソッドのMDEが記述していない内容の具体的なエリアにアクセスする権限がユーザに認められていないのなら、イベントを原子エレメントにマッピングしそこなうことがある。このメカニズムは、例えば、内容の断片のカスタマイズされたバージョンを配付するのに用いることができ、また、ユーザに配送されるEVENTメソッドのMDEを改変することによって、その内容オブジェクトにおけるさまざまなバージョンへのアクセスを制御するのに用いることができる。

この技術の具体的な使用法としては、内容のある断片について異なるさまざまな言語（例えば、英語、フランス語、スペイン語）によるバージョンの配付を制御することが挙げられよう。

課金

図53cは、BILLINGメソッド1980によりおこなわれる処理制御ステップの一例を示すフローチャートである。BILLINGメソッドの例は、既に説明した図49d、図50dおよび図51dにも述べられている。図53cに示されているBILLINGメソッド1980は、上記例よりもいくらか一般化されている。上述した例のBILLINGメソッドと同様に、BILLINGメソッド1980も、計量値を受け取って、課金すべき金額を決定する。BILLINGメソッド1980はまず、（もし必要なら）適切な情報をBILLINGメソッドの監査追跡UDEに書き込むことによって、BILLING監査追跡を予めおこなう（ブロック1982、1984）ことができる。その後、BILLINGメソッド1980は、安全データベースからBILLINGメソッドのマップDTDを得て、ロードする（ブロック1985、1986）ことができる。このマップは、このBILLINGメソッドにより用いられるべきBILLINGメソッドのマップMDE（例えば、価格リスト、表、あるいは課金額計算アルゴリズムに対するパラメータ）を記述している。BILLINGメソッドのマップMDEは、内容オブジェクトの一部としても、あるいは、登録時に制御情報と組みあ

わされる、別々に配送可能な成分としても、配送されうる。

BILLINGメソッドのマップMDEは、この例では、このBILLINGメソッドにおいて用いられるべき価格決定アルゴリズム（例えば、放出された内容の１バイトにつき0.001ドルの課金）を記述することができる。ブロック1988（「計量値を課金額にマッピングする」）は、EVENTメソッドのブロック1950と同様に作用する。すなわち、このブロックは、計量値を課金価格にマッピングする。処理ステップ1988は、また、安全データベース（プライバシーフィルタにより制限されている）に問い合わせることによって、その他のオブジェクトまたは情報（例えば、ユーザ情報）が、BILLINGメソッドのアルゴリズムの一部として存

在してかどうかを判定する。

その後、BILLINGメソッド1980は、もし必要なら、BILLING監査追跡を、BILLINGメソッドの監査追跡UDEに書き込み（ブロック1990、1992）、課金額をコールしているCONTROLメソッド（あるいはその他の制御処理）へとリターンする準備をすることができる。しかし、その前に、BILLINGメソッド1980は、課金額が決定されたかどうかをテストすることができる（判定ブロック1994）。もし決定された課金額がなかったら、BILLINGメソッドは失敗することがある（ブロック1996）。このことは、もし、BILLINGメソッドのMDEが記述する価格決定テーブルの具体的なエリアにアクセスする権限がユーザに認められていない（例えば、この内容オブジェクトから100.00ドルを超えない情報なら購入できることがある）のなら、生じることがある。

アクセス

図54は、ACCESSメソッド2000によりおこなわれるプログラム制御ステップの一例を示すフローチャートである。上述したように、ACCESSメソッドは、オブジェクト300に埋め込まれている内容にアクセスする、すなわち書き込み、読み出し、またはその他の操作あるいは処理を施すために用いられうる。多くの場合、このACCESSメソッドは比較的、簡単でありうる。なぜなら、オブジェクトは、例えば、容易にアクセス可能なローカル記憶装置に格納されうるからである。しかし、一般的な例では、ACCESSメソッド2000は、オブジェクトを得るために、もっと

複雑なプロシージャを経なければならない。例えば、あるオブジェクト（あるいはオブジェクトの一部）が、リモートサイトでしか入手できず、リアルタイムのダウンロードまたはフィードのかたちで提供されることがある（例えば、ブロードキャスト伝送の場合）。たとえ、そのオブジェクトがVDEノードに局所的に格納されるとしても、このオブジェクトは、コールしている処理に直接、アクセスできないように、安全なオブジェクト、つまり保護されたオブジェクトとして格納されうる。ACCESSメソッド2000は、オブジェクトにアクセスするのに必要とされる接続、ルーティングおよび安全上の各種要件を確立す

る。これらのステップは、コールしている処理が、アクセスリクエストを発しさえすればよいように、また、そのオブジェクトまたはオブジェクトのクラスに対応する特定のACCESSメソッドが、そのオブジェクトに実際にアクセスする際に伴う詳細およびロジスティクス（logistics）のすべてを操作できるように、コールしている処理に対してトランスペアレントにおこなわれてもよい。

ACCESSメソッド2000は、まず、（もし必要なら）、ACCESS監査追跡UDEへと書き込むことによって、ACCESSの監査追跡を予めおこなうことができる（ブロック2002、2004）。次に、ACCESSメソッド2000は、ACCESS MDEのフォーマットを決定するために、ACCESSメソッドのDTDを読み出し、ロードすることができる（ブロック2006、2008）。ACCESSメソッドのMDEは、好ましい実施の形態では、アクセスされる特定のオブジェクトについての、ソースおよびルーティング情報を指定する。ACCESSメソッドのDTDを用いて、ACCESSメソッド2000は、（例えば、電話番号、アカウントID、パスワードおよび／またはリモート資源依存言語によるリクエストスクリプトにより）訂正パラメータをロードすることができる。

ACCESSメソッド2000は、安全データベースからACCESSメソッドのMDEを読み出し、それをACCESSメソッドのDTDに従って読み、そしてこのMDEに基づいて、暗号化された内容ソースおよびルーティング情報をロードする（ブロック2010、2012）。このソースおよびルーティング情報は、暗号化された内容のロケーションを指定する。その後、ACCESSメソッド2000は、この内容に対する接続が利用可能であるかどうかを判定する（判定ブロック2014）。この「接続」は、例えば、リモート

サイトへのオンライン接続でも、リアルタイムの情報フィードでも、例えば安全な／保護された資源へのパスであってもよい。もしこの内容に対する接続が現在、利用可能ではないのなら（判定ブロック2014に対する「ノー」エグジット）、ACCESSメソッド2000は、その接続をオープンするためのステップをおこなう（ブロック2016）。もし（例えば、保護された安全な資源にアクセスする権限がユーザに認められていないために）接続に失敗すれば、ACCESSメソッド2000は、失敗を表示してリターンする（終端点

2018）。一方、オープン接続に成功すれば、ACCESSメソッド2000は、暗号化された内容を得る（ブロック2020）。その後、ACCESSメソッド2000は、もし必要なら、ACCESS監査追跡を安全データベースのACCESSメソッドの監査追跡UDEに書き込んだ（ブロック2022、2024）後、終了する（終端点2026）。

復号化および暗号化

図55aは、好ましい実施の形態により提供されるDECRYPTメソッド2030の代表例によりおこなわれる処理制御ステップの一例を示すフローチャートである。好ましい実施の形態では、DECRYPTメソッド2030は、適切なPERC 808から復号化鍵を得るか、または引き出し、それを用いて暗号化された内容の１ブロックを復号化する。DECRYPTメソッド2030には、暗号化された内容の１ブロック、またはその暗号化されたブロックが格納されている場所を示すポインタが渡される。DECRYPT 2030は、鍵ブロックから鍵番号を選択する（ブロック2032）。安全のために、内容オブジェクトは、１つよりも多くの鍵を用いて暗号化されてもよい。例えば、映画は、その最初の10分間のあいだは第１の鍵を用いて暗号化され、次の10分間のあいだは第２の鍵を用いて暗号化されてもよい（以下も同様）。これらの鍵は、PERC 808内の「鍵ブロック」と呼ばれる構造に格納される。この選択処理は、内容を復号化するために、その鍵ブロックから用いるべき正しい鍵を判定することを伴う。この選択のための処理は、イベントを原子エレメント番号にマッピングするためにEVENTメソッドにより用いられる処理に類似している。DECRYPTメソッド2030は、その後、安全データベース610から適切なPERC 808にアクセスし、PERCから鍵（または「シード」）をロードすることができる（ブロック2034、2036）。

この鍵情報は、内容を復号化するのに用いられる実際の復号化鍵であってもよいし、復号化鍵の少なくとも一部の導出、計算を可能にする情報であってもよい。もし必要なら、DECRYPTメソッド2030は、ブロック2034においてPERC 808から読み出された情報に基づいて、復号化鍵を計算する（ブロック2038）。その後、DECRYPTメソッド2030は、このようにして得られた、および／または計算された復号化鍵を用いて、暗号化された情報のブロックを実際に復号化する（ブロック2040）。DECRYPTメソッド2030は、復号化されたブロック（または、それがどこで見つけられるかを示すポインタ）を出力して、終了する（終端点2024）。

図55bは、ENCRYPTメソッド2050の代表例によりおこなわれる処理制御ステップの一例を示すフローチャートである。ENCRYPTメソッド2050には、入力として、暗号化すべき情報の1ブロック（または、それがどこで見つけられるかを示すポインタ）が渡される。次に、ENCRYPTメソッド2050は、鍵ブロックから用いるべき暗号化鍵を決めることができる（ブロック2052）。暗号化鍵の選択に際しては、書き込まれるべき内容のある具体的なブロックに対する鍵が、PERC 808に格納されている鍵ブロックに既に存在しているかどうかを判定する。もしその鍵が既に鍵ブロック内に存在しているのなら、適切な鍵番号が選択される。もしそのような鍵が鍵ブロックには存在しないのなら、暗号化アルゴリズムに適したアルゴリズムを用いて、新しい鍵が計算される。この鍵は、その後、DECRYPTメソッド2030が、その鍵にアクセスして、その内容オブジェクトに格納されている内容を復号化できるように、PERC 808の鍵ブロック内に格納される。その後、ENCRYPTメソッド2050は、適切なPERCにアクセスすることによって、情報ブロックを暗号化するのに用いられる暗号化鍵を得、導出し、および／または計算する（図55aのブロック2034、2036、2038に類似するブロック2054、2056、2058）。その後、ENCRYPTメソッド2050は、得られたおよび／または導出された暗号化鍵を用いて情報ブロックを実際に暗号化し（ブロック2060）、その後、終了する（終端点2062）前に、暗号化された情報ブロックまたはそれがどこで見つけられるかを示すポインタを出力する。

内容

図５６は、好ましい実施の形態により提供されるCONTENTメソッド２０７０の代表例によりおこなわれる処理制御ステップの一例を示すフローチャートである。CONTENTメソッド２０７０は、好ましい実施の形態では、安全処理を用いて、保

護されている内容の「一覧表」を作成する。例えば、CONTENTメソッド２０７０は、安全な内容から安全ではない（「公開の」）情報を引き出すのに用いられうる。引き出されたこのような公開情報としては、例えば、要約、索引、内容一覧、ファイルのディレクトリ、内容が利用可能になるスケジュール、あるいは、例えば映画の「予告編」のような抜粋がある。

CONTENTメソッド２０７０は、まず始めに、提供され、引き出されるべき内容が、安全な内容から引き出されなければならないのか、あるいは、その内容は、スタティックな値のかたちで既にオブジェクト内で利用可能であるかを判定する（判定ブロック２０７０）。いくつかのオブジェクトは、例えば、明らかにCONTENTメソッド２０７０により抽出される目的で提供される、予め格納された要約、索引、内容一覧などを含んでいることがある。もしオブジェクトがそのようなスタティックな値を含んでいるのなら（判定ブロック２０７２に対する「スタティック」エグジット）、CONTENTメソッド２０７０は、単にこのスタティック値の内容情報をオブジェクトから読み出し（ブロック２０７４）、望みとあれば復号化した後、この内容記述を明らかにする（ブロック２０７６）。一方、もしCONTENTメソッド２０７０が、この一覧表／内容記述を安全なオブジェクトから引き出さなければならないのなら（判定ブロック２０７２に対する「引き出し」エグジット）、CONTENTメソッドは、一覧表アルゴリズムに従って、入れ物から情報を安全に読み出し、一覧表を作成することができる（ブロック２０７８）。

抽出および埋め込み

図５７ａは、好ましい実施の形態により提供されるEXTRACTメソッド２０８０の代表例によりおこなわれる処理制御ステップの一例を示すフローチャートである。EXTRACTメソッド２０８０は、あるオブジェクトから内容をコピーまたは抜き出し、その内容を新しいオブジェクトに入れるのに用いられる。好ましい実施の形態では、EXTRACTメソッド２０８０は、内容を明らかにすることを全く伴わず、単にある入れ

物から内容を取り出して、別の入れ物に入れるだけである。ここで、これらの入れ物は、ともに安全でありうる。内容の抽出が明らかにすることと異

なるのは、その内容が、決して安全な入れ物の外部に曝されることがないことである。抽出と埋め込みとは、相補的な機能である。すなわち、抽出では、内容をある入れ物から取り出し、抽出されたその内容と、その内容に関連づけられた何らかの具体的な制御情報とを含む新しい入れ物をつくる。これに対して、埋め込みでは、既にある入れ物の中にある内容を取り出し、それ（つまり、その完全なオブジェクト）を、直接および／または参照の上、別の入れ物に格納し、現存する内容に関連づけられた制御情報を、新しい内容の情報と一体化する。

EXTRACTメソッド2080は、まず始めに、監査UDEを予めおこなう（ブロック2082、2084）。次に、EXTRACTメソッドは、BUDGETメソッドをコールし、ユーザが、内容をオリジナルオブジェクトから抽出するのに十分な予算をもっているか（そしてその権利が認められているか）を確かめる（ブロック2086）。もしユーザの予算がこの抽出にパーミッションを与えないのなら（判定ブロック2088に対する「ノー」エグジット）、EXTRACTメソッド2080は、失敗監査追跡を書いて（ブロック2090）、終了する（終端点2092）。もしユーザの予算がこの抽出にパーミッションを与えるのなら（判定ブロック2088に対する「イエス」エグジット）、EXTRACTメソッド2080は、具体的規則および制御情報を含む、抽出されたオブジェクトのコピーを作成する（ブロック2094）。好ましい実施の形態では、このステップは、そのコピーを実際に制御するメソッドをコールすることを伴う。このステップは、例えば、オリジナルオブジェクトに関連づけられた特定のPERC 808次第では、復号化および暗号化を伴うことも、伴わないこともある。次に、EXTRACTメソッド2080は、開始すべき抽出を承認する権利によって、制御の何らかの変更にパーミッションが与えられるかどうかをチェックする（判定ブロック2096）。いくつかのケースでは、抽出権を得るためには、オリジナルオブジェクトに関連づけられたPERC 808（または、この目的で含められたPERC）の正確なコピーを、新しい（デスティネーションの）入れ物に入れることが要求されることがある（判定ブロック2096に対する「ノー」エグジット）。もし制御の変更にパーミッションが与えられな

いのなら、抽出メソッド2080は、終了する（終端点2102）前に、単に監査情報を

監査UDE

に書き込む（ブロック2098、2100）だけである。一方、もし抽出権が、ユーザに対して、制御変更のパーミッションを与えるのなら（判定ブロック2096に対する「イエス」）、EXTRACTメソッド2080は、（例えば、ユーザから、抽出権を発生／許可した配付者から、またはその他の何らかのソースからの）新しい、つまり変更された制御情報をユーザから請求するメソッドまたはロードモジュールをコールすることができる（ブロック2104、2106）。EXTRACTメソッド2080は、その後、メソッドまたはロードモジュールをコールすることによって、ユーザの指定したこれらの制御情報を反映した新しいPERCを生成することができる（ブロック2104）。この新しいPERCは、新しい（デスティネーション）オブジェクトに入れられ、監査ステップがおこなわれた後、処理は終了する。

図57bは、好ましい実施の形態により提供されるEMBEDメソッド2110の代表例によりおこなわれる処理制御ステップの一例である。EMBEDメソッド2110は、図57aに示されているEXTRACTメソッド2080に似ている。しかし、EMBEDメソッド2110は、わずかに異なる機能を果たす。すなわち、このメソッドは、オブジェクト（または参照）をデスティネーションの入れ物に書き込む。図57bに示されているブロック2112～2122は、図57aに示されているブロック2082～2092に類似している。ブロック2124において、EMBEDメソッド2110は、ソースオブジェクトをデスティネーションの入れ物に書き込む。また、同時に、このデスティネーションの入れ物の制御情報を抽出したり、変更したりしてもよい。ある選択肢としては、ただデスティネーションの入れ物の制御情報のみをそのままにしておき、オリジナルの入れ物の制御情報に加えて、埋め込まれているオブジェクトに関連づけられた制御情報のセットのすべてを含ませるというやりかたがある。しかし、最適化のために、好ましい実施の形態では、現在、埋め込まれているオブジェクトに関連づけられた制御情報が「要約され」、デスティネーションの入れ物の制御情報内に取り込まれるようにする技術を提供する。ブロック2124は、この制御情報を要約するか、または変更するメソッドをコールすることができる。次に、EMBEDメ

ソッド２１１０は、図５７ａに示されているステップ２０９６、２１０４および２１０６に類似するステップ２１２６～２１３０をおこなう

ことによって、もし承認されれば、ユーザが、埋め込まれたオブジェクトおよび／またはデスティネーションの入れ物に関連づけられた制御情報を変更および／または指定できるようにする。そして、ＥＭＢＥＤメソッド２１１０は、終了する（終端点２１３６）前に、監査情報を監査ＵＤＥに書き込む（ブロック２１３２、２１３４）。

曖昧化

図５８ａは、好ましい実施の形態により提供されるＯＢＳＣＵＲＥメソッド２１４０の代表例によりおこなわれる処理制御ステップの一例を示すフローチャートである。ＯＢＳＣＵＲＥメソッド２１４０は、典型的には、安全な内容を、価値を減じた（ｄｅｖａｌｕｅｄ）形態で明らかにするために用いられる。例えば、ＯＢＳＣＵＲＥメソッド２１４０は、視聴者がイメージを識別することはできるが、その完全な価値を享受することはできないように、高解像度のイメージを低解像度で放出することができる。別の例としては、ＯＢＳＣＵＲＥメソッド２１４０は、イメージの上にわたってそれを曖昧にするラベル（例えば、「ＣＯＰＹ」、「ＰＲＯＯＦ」など）を置くことにより、その価値を曖昧にする。ＯＢＳＣＵＲＥメソッド２１４０は、テキスト、イメージ、オーディオ情報あるいはその他のタイプの内容を「曖昧にする」ことができる。

ＯＢＳＣＵＲＥメソッド２１４０は、まずＥＶＥＮＴメソッドをコールし、その内容が曖昧化するのに適しているか、そしてその範囲にあるかどうかを判定する（ブロック２１４２）。もしこの内容が曖昧にするのに適していないのなら、ＯＢＳＣＵＲＥメソッドは終了する（判定ブロック２１４４の「ノー」エグジット、終端点２１４６）。この内容が曖昧にされるべきであるとする（判定ブロック２１４４に対する「イエス」エグジット）と、ＯＢＳＣＵＲＥメソッド２１４０は、この内容を不明瞭にするために以前にコールされたことがあるかどうかを判定する（判定ブロック２１４８）。ＯＢＳＣＵＲＥメソッド２１４０がこのオブジェクト／内容のために以前にコールされたことがないものとすると（判定ブロック２１４８に対する「イエス」エグジット）、ＯＢＳＣＵＲＥメソッド２１４０は、適切なＯＢＳＣＵＲＥメソッドのＭＤＥ

を安全データベースから読み出し、曖昧化の式および／またはパターンをMDEからロードする（ブロック2150、2152）。その後、OBSCUREメソッド2140は、ブロック2150によりロードされたパターンおよび／または式に基づいて、適切な曖昧化変換を施す（ブロック2154）。そして、OBSCUREメソッドは終了することができる（終端ブロック2156）。

指紋

図58bは、好ましい実施の形態により提供されるFINGERPRINTメソッド2160の代表例によりおこなわれる処理制御ステップの一例を示すフローチャートである。好ましい実施の形態では、FINGERPRINTメソッド2160は、明らかにされた内容に、誰がその内容を明らかにしたかを示す「指紋」識別子を「マーク」し、および／またはそのようなマークをチェックするように作用する。これにより、内容を調べることによって、誰が安全にされていない内容を明らかにしたかを後に判定することが可能になる。FINGERPRINTメソッド2160は、例えば、オーディオ、ビデオあるいは２進フォーマットの情報を表現するデータストリーム内にユーザIDを挿入することができる。FINGERPRINTメソッド2160は、FINGERPRINTメソッドのブロック2174により施される変換が、明らかにされた内容を曖昧にするのではなく、それに「指紋をつける」という点を別にすれば、図58aに示されているOBSCUREメソッド2140によく似ている。

図58cは、明らかにされた内容、および／または明らかにされた日時、および／または明らかにされた内容のその他の識別基準をリクエストした、オブジェクト、および／またはプロパティ、および／またはユーザを識別する「指紋」2161を明らかにされた内容に挿入する、「指紋刻印」プロシージャ2160の一例を示している。

このような指紋2161は、「埋もれさせる」ことができる。すなわち、ファイルのフォーマット、挿入アルゴリズムの精巧さおよび／または多様性、およびオリジナルの指紋の印されていない内容（（１つ以上の）アルゴリズムの逆エンジニアリングについての比較のため）に依存して、典型的なユーザ、高度な「ハッカー」および／またはすべてのユーザから指紋を隠すように挿入される。挿入さ

れた、あるいは埋め込まれた指紋2161は、好ましい実施の形態では、より安全にするために、少なくとも部分的には暗号化されてもよい。このように暗号化された指紋2161は、「平明な」（平文）の形式で与えられた、明らかにされた内容の中に埋め込まれうる。

指紋2161は、多種多様な目的のために用いられうる。そのような目的には、例えば、明らかにされたマテリアルの誤用を実証したり、明らかにされた内容のソースを実証したりするといったしばしば相互に関連する目的が含まれている。ソフトウェアのプライバシーは、指紋の刻印が非常に有用になりうる好例である。また、指紋刻印は、映画や、オーディオ記録や、マルチメディアや、情報データベースや、伝統的な「文学系の」素材などを含む、ほとんどのタイプの電子的に配送される情報について、内容プロバイダの権利を守らせる一助になりうる。指紋刻印は、著作権保護の代替としても、あるいはそれを補強するものとしても望ましい。

ソフトウェアアプリケーションの著作権侵害は、たいていの場合、ある個人が、当該個人の所有する別のコンピュータで使用するために違法コピーを作成するときに発生するのではなく、むしろコピーをサードパーティに与える場合に発生する。これにより、違法コピーの連鎖（より正確に言えば、ピラミッド）がスタートすることがしばしばある。なぜなら、コピーは、個人から個人へと手渡されていくからである。指紋2161を埋め込ませることで身元が判明する結果になることを恐れると、（現在でも、多くの人がそうであるように）たいていの個人は、広く行き渡る「カジュアルな」著作権侵害への参加を思いとどまることになりやすい。あるケースでは、内容は、指紋刻印メソッドにより指紋の存在についてチェックされることによって、内容プロバイダの権利を守らせる一助とすることがある。

異なる複数の指紋2161により、異なる複数のレベルの安全性を保つことができる（例えば、ある指紋2161（1）は、営利団体により判読可能／識別可能であるが、別の指紋2161（2）は、より信頼性の高いエージェンシーだけが判読可能

てありうる）。より安全性の高い指紋2161を生成するためのメソッドは、より複

雑な暗号化技術（例えば、ディジタル署名）および／または位置検出方法論（location methodologies）の曖昧化を用いることができる。２つ以上の指紋2161をそれぞれ異なる位置に埋め込ませること、および／または異なる複数の技術を用いることは、指紋の刻印された情報をハッカーから保護する一助になる。より安全性の高い指紋を提供するために用いられる技術が、望ましくない量の過剰負荷をもたらすのなら、より安全性の高い指紋は、内容の明らかにされるたびではなく、むしろ周期的に用いられてもよい。とはいうものの、毎回用いるほうが有効でありうる。なぜなら、指紋刻印の主要な目的は、抑止（すなわち、違法コピーを作成する側の、そのコピーが発覚するのではないかという懸念による抑止）にあるからである。

例えば、承認済みのパーティ（例えば、配付者、サービスパーソネル、クライアント管理者、あるいはVDE電子器具600を用いる情報交換所）であれば、容易に識別できるような指紋2161の複製を埋め込むことがあるかもしれない。また、ある指紋2161について１つ以上の追加コピーあるいは変形（例えば、関連する識別情報の一部または全部を記述する情報を有する指紋）を埋め込むかもしれない。その場合、これら１つ以上の追加の指紋2161は、より安全性の高いメソッドで維持されうる。

指紋刻印は、また、プライバシー関連事項も保護することができる。例えば、指紋2161を識別するのに必要なアルゴリズムおよび／またはメカニズムは、特に高信頼のエージェントを通してのみ利用可能とすることができる。

指紋刻印2161は、多くの形態をとりうる。例えば、イメージの場合、（イメージ全体、またはそのイメージの１サブセットにわたって広がっている）Ｎ個の画素ごとの色を（少なくとも、通常の、何の手段もない観察者には）視覚的に認識できないように、微妙にシフトさせることができる。これらのシフトは、（オリジナルのイメージにアクセスしても、しなくても）イメージを分析することによって解釈可能である。ここで、１回ごとに発生する、または発生しない色（または階調）のシフトは、ディジタル情報記憶での１つ以上の２進「オンまたはオフ」ビットに相当する。また、Ｎ個の画素は、所定の順序（consistent）で並ん

でいてもよいし、あるいは疑似ランダム的に（とはいうものの、少なくとも部分的には、オブジェクト作成者、オブジェクトプロバイダ、クライアント管理者および／またはVDE管理者により解釈可能なように）並んでいてもよい。

また、アプリケーションによっては、同様の利益を生む（すなわち、ソース情報のある種の修正の結果、通常は認識不可能な形態で情報を格納すること）その他のイメージ（つまり動画、オーディオなど）の修正が適切であることもある。例えば、格納されているオーディオ情報の周波数を何らかのかたちで微妙に変調すれば、この周波数は、通常は聴取者に認識不可能であるが、それでも正しいツールを用いれば判別可能であるように修正することができる。情報記憶のある種の特性は、同様の結果を達成できるように光学的に格納されたある情報の極性を、微妙だが解釈可能な範囲内で変化させるように、修正可能である。その他の電子的、磁気的、および／または光学的特性を利用したその他の変化を利用することもできる。

グラフィカルフォーマットを用いるファイル（例えば、マイクロソフトウィンドウズワードプロセシングファイル）に格納されている内容は、指紋2161を「埋もれさせる」のに有意な機会を提供する。イメージおよび／またはオーディオを含む内容は、アクセス権限のない個人が識別するのは困難であるような指紋2161を埋め込ませる機会を提供する。なぜなら、比較のために用いられる「指紋刻印されていない」オリジナルがない場合には、オリジナルの性格が通常は未知であり、イメージおよび音声データの両方ともに大量のデータが用いられている（このような場合、ごく小さい変化には特に敏感なわけではない）のであるから、オーディオ周波数の１つ以上の時間事例において、あるいは１つ以上のビデオイメージなどにおいて微妙でごく小さい変化を施したとしても、そのような変化自体は、通常、識別不可能である。フォーマットされたテキスト文書、特にグラフィカルワードプロセッサ（例えば、マイクロソフトウィンドウズあるいはアップルマッキントッシュワードプロセッサ、およびそれらのDOSおよびUnix版の等価物など）を用いて作成された文書の場合、指紋2161は、通常、エンド

ユーザには通常不可視である文書データ表現の一部（ヘッダフィールドあるいは

その他の表示されないデータフィールド）に目立たないかたちで挿入されうる。

さらに別の形態の指紋刻印（いくつかのテキスト文書には特に好適でありうる）は、文字の形状をある与えられたフォントについて利用し、制御する。個々の文字は、ある種の「指紋」情報を包含する、わずかに異なる視覚的形状をもつことができる。ある与えられた文字の形状のこのような変形は、通常は識別不可能である。これは、一つには、異なる別々の供給者から入手可能な同一フォントの複数のバージョンには、わずかな変化が多数見受けられるからであり、また、一つには、そのような変化がごく小さいものであるからである。例えば、好ましい実施の形態では、Adobe Type Alignのようなプログラムを用いることができる。このプログラムは、そのオフザシェルフバージョンでは、ユーザがフォント文字を多種多様なメソッドで修正できるようにする能力をサポートしている。フォント文字の数学的定義がユーザの命令により修正されることによって、具体的な修正セットが文字またはフォントに施されるようになる。情報の内容は、通常の状況ではユーザが認識するにはあまりにも微細ではあるが、それでも指紋2161を適切に符号化可能とするかたちで一部またはすべての文字を修正できるように、（ユーザの選択に対する一選択肢として）アナログ的に用いられてもよい。ある与えられた文字の多種多様な微妙に異なるバージョンを単一の文書内に用いることによって、取引に関連し、フォントにより指紋刻印された情報をもつ能力の向上が可能になる。

指紋刻印のためのアプリケーション例としては、他にも以下のようなものがある。

１．ソフトウェアプログラムにおいて、多少なりとも同一性の高い動作を生じるように、しかし分析すれば、指紋情報を詳細に示す差を生じるように、いくつかの相互に置換可能なコード断片を選択すること。

２．データベースを用いて、いくつかのフィールド（例えば、日付など）が様々に異なるしかたで現れるようにフォーマットする選択をおこなうこと。

３．ゲームで、背景を調整したり、いくつかのイベントの順序を変更したりすること。ゲームの各種要素のタイミングおよび／または出現順序を認識可能なか

たちで、あるいはごく微妙に変化させること、あるいは、ゲームの各種要素の外見をわずかに変化させることもこれに含まれる。

指紋刻印メソッド2160は、（もしおこなわれるとすれば）典型的には、内容が内容オブジェクト300から明らかにされる時点でおこなわれる。しかし、依然として暗号化された形態であるままで内容に「マークをつける」ために、オブジェクトの配付後、ただちにおこなわれてもよい。例えば、ネットワークベースのオブジェクト格納場所は、あるオブジェクトをリクエスト者に送信する前に、そのオブジェクトの内容に指紋2161を埋め込ませることができる。その場合、指紋情報は、内容のリクエスト者／エンドユーザを識別可能とする。このことは、承認を得ずに内容を明らかにするのに用いられる「偽物の」電子器具600を検出する一助になる。

破壊

図59は、好ましい実施の形態により提供されるDESTROYメソッド2180によりおこなわれる代表例によりおこなわれる処理制御ステップの一例を示すフローチャートである。DESTROYメソッド2180は、オブジェクトにアクセスするためにユーザがリクエストするURTを破壊することによって、ユーザがそのオブジェクトを使用する能力を奪う。好ましい実施の形態では、DESTROYメソッド2180は、まず、監査情報を監査UDEに書き込む（ブロック2182、2184）ことができる。その後、DESTROYメソッド2180は、WRITEおよび／またはACESSメソッドをコールし、オブジェクトのヘッダおよび／またはその他の重要な部分を劣化させ（よって破壊もする）情報を書き込む（ブロック2186）。DESTROYメソッド2180は、その後、適切な情報を制御構造に書き込むことによってダメージを受けた制御構造（例えば、URT）の１つ以上にマークをつけることができる（ブロック2188、2190）。最後に、DESTROYメソッド2180は、終了する（終端点2196）前に、追加の監査情報を監査UDEに書き込むことができる（ブロック2192、2194）。

パニック

図60は、好ましい実施の形態により提供されるPANICメソッド2200の代表例によりおこなわれる処理制御ステップの一例を示すフローチャートである。PANIC

メソッド2200は、安全性の侵害が検出された時に、コールされうる。PANICメソッド2200は、例えば、現在、オブジェクトにアクセスするのに用いられているチャネルを破壊し、かつダメージを受けた時のユーザおよびオブジェクトに関連づけられた制御構造（例えば、URT）の１つ以上にマークをつけることによって、ユーザが、現在、アクセスしているオブジェクトにそれ以上アクセスできないようにすることができる（それぞれ、ブロック2206および2208～2210）。制御構造がダメージを受けているので、VDEノードは、ユーザが同じオブジェクトに再びアクセスできるようになる前に、（１つ以上の）有効な制御構造を得ることができるように、管理者にコンタクトをとる必要がある。VDEノードが管理者にコンタクトをとる時、管理者は、安全性の侵害が起こらないと安心できるのに十分な情報をリクエストすることができる。もし安全性の侵害が起こったのなら、そのような安全性侵害が繰り返されないことを保証するための適切なステップを講じる。

計量

図61は、好ましい実施の形態により提供されるMETERメソッドの代表例によりおこなわれる処理制御ステップの一例を示すフローチャートである。METERメソッドについては、図49、図50および図51を参照して既に説明したが、図61に示されているMETERメソッド2220は、おそらく、それよりもいくらか代表的な例である。好ましい実施の形態では、METERメソッド2220はまず、METER監査追跡UDEにアクセスすることによって、監査追跡を予めおこなう（ブロック2222、2224）。その後、METERメソッド2220は、安全データベースから計量UDE用のDTDを読み出すことができる（ブロック2226、2228）。METERメソッド2220は、その後、安全データベースから計量UDEを

読み出すことができる（ブロック2230、2232）。次に、METERメソッド2220は、得られた計量UDEをテストすることによって、それが失効しているかどうかを判定する（判定ブロック2234）。好ましい実施の形態では、それぞれの計量UDEには、失効の日付がマークされうる。もし現在の日付／時刻が、計量UDEの失効日よりも後であれば（判定ブロック2234に対する「イエス」エグジット）、METERメソッ

ド2220は、失敗を監査記録に記録し、失敗状態を示して終了する（ブロック2236、2238）。

計量UDEがまだ失効していないものとすると、計量メソッド2220は、原子エレメントと、例えば、EVENTメソッドからMETERメソッドに渡されたイベントカウントとを用いて、それを更新することができる（ブロック2239、2240）。METERメソッド2220は、その後、（終端点2246で）終了する前に、計量使用監査記録を、計量監査追跡UDEに保存することができる（ブロック2242、2244）。

好ましい実施の形態により提供されるその他の安全性特徴

好ましい実施の形態により提供されるVDE 100は、「強行攻撃（brute force attack）」の成功の場合以外は、安全性が侵犯されることがないことを保証する助けとなるのに十分な安全性を有している。よって、そのような「強行攻撃」に成功するだけの時間およびコストは、実質的に導き出されるどの値も超えている。加えて、VDE 100により提供される安全性は、VDEの内部のはたらきを区分する。よって、「強行攻撃」に成功しても、全システムではなく、保護されている情報のうち厳密に境界の定められた1サブセットのみが侵犯されるだけである。

以下は、好ましい実施の形態により提供される安全性の局面および特徴の中からいくつかを挙げたものである。

- PPE 650の安全性およびそれがおこなう処理
- 安全データベース610の安全性
- PPE 650によりおこなわれる暗号化／復号化の安全性
- 鍵の管理、暗号化／復号化鍵および共有される秘密の安全性
- 認証／外部通信の安全性
- 安全データベースバックアップの安全性
- 電子器具600間のVDE内部情報の安全な伝搬能力
- VDE安全情報にアクセスするパーミッションの安全性
- VDEオブジェクト300の安全性
- VDE安全性の完全性

このような安全性の局面および考察のうちいくつかについては、既に説明した

。以下では、他の箇所では十分に取り扱っていない、好ましい実施の形態による安全性の特徴についてさらに詳しく議論する。

鍵の管理および共有される秘密

VDE100は、安全性を確保するために、鍵と、共有される秘密とを用いる。好ましい実施の形態では、鍵の使用について以下の特徴が実現される。

・　異なる暗号化システム／鍵のタイプ

・　安全な鍵の長さ

・　鍵の発生

・　鍵の「旋回」および鍵の「老化(aging)」

これらのタイプのそれぞれについて以下に説明する。

Ａ．公開鍵および対称鍵暗号化システム

本質を隠すために情報を隠匿したり、変換したりする処理は、暗号化と呼ばれる。暗号化により、「暗号文」が生じる。暗号文から本質を復元するための、暗号化処理とは逆の処理は、「復号化」と呼ばれる。暗号化アルゴリズムは、暗号化および復号化のために用いられる数学的関数である。

最も現代的な暗号化アルゴリズムでは、「鍵」を用いる。この「鍵」は、提供される変換系列(family)のうちの一つを指定する。鍵によって、標準的で、公開されており、既に試験済みの暗号化アルゴリズムを用いながら、このアルゴリズムを用いておこなわれる具体的な変換を確実に秘密のままにしておくことができる。このように、特定の変換の秘密性は、アルゴリズムの秘密性にではなく、鍵の秘密性に依存している。

鍵に基づくアルゴリズムには、大まかに分けると以下の２つの形態がある。好ましい実施の形態によるPPE 650では、これらのうちの一方または両方を用いることができる。

対称鍵、および

公開鍵(「PK」)

対称アルゴリズムは、暗号化鍵が復号化鍵から計算されうる(かつ逆も同様な)アルゴリズムである。このような多くのシステムでは、暗号化鍵と復号化鍵と

は同じである。「シークレット鍵(secret-key)」アルゴリズム、「単一の鍵」アルゴリズムあるいは「共有される秘密」アルゴリズムとも呼ばれるこれらのアルゴリズムは、送り手により作成された暗号文が受け手により復号化される前に、送り手および受け手の両方が鍵について同意することを要求する。この鍵は、秘密のままにしておかなければならない。対称アルゴリズムの安全性は、鍵に存する。この鍵を外部に漏らすことは、このような暗号化システムでは、誰でも情報を暗号化し、復号化できるようになることを意味している。SchneierのApplied Cryptography、第３頁を参照のこと。好ましい実施の形態で使用可能な対称鍵アルゴリズムの例をいくつか挙げれば、DES、Skipjack/Clipper、IDEA、RC2およびRC4がある。

公開鍵暗号化システムでは、暗号化に用いられる鍵は、復号化に用いられる鍵とは異なる。さらに、一方の鍵を他方の鍵から導き出すことは、計算的に実行不可能である。これらの暗号化システムにおいて用いられるアルゴリズムが「公開鍵」と呼ばれるのは、これら２つの鍵の一方が、他方の鍵の安全性を危うくすることなく、公にされうるからである。また、時には、それらは「非対称」暗号化システムと称される。なぜなら、それらのシステムは、暗号化と復号化でそれぞれ異なる鍵を用いるからである。公開鍵アルゴリズムとしては、例えば、RSA、El GamalおよびLUCがある。

好ましい実施の形態によるPPE 650は、対称鍵暗号化システムのみに基づいて、公開鍵暗号化システムのみに基づいて、もしくは対称鍵暗号化システムおよび公開鍵暗号化システムの両方に基づいて、動作することができる。VDE 100には、何か特殊な暗号化アルゴリズムが必要になるわけではない。好ましい実施の形態により提供されるアーキテクチャは、PKおよび／またはシークレット鍵（非PK）アルゴリズムを含む多数のアルゴリズムをサポートできる。あるケースでは、暗号化／復号化アルゴリズムの選択は、コスト、市場の需要、その他の市販されているシステムとの互換性、輸出法のようなビジネス上のさまざまな判断に依存することになる。

好ましい実施の形態は、特定のタイプの暗号化システムには依存せず、（１つ

以上の）暗号化／復号化アルゴリズムにも依存しないが、好ましい例では、PPE 650間の安全な通信のためにPK暗号化システムを用い、VDEオブジェクト300間の「膨大な」暗号化／復号化のためにはシークレット鍵暗号化システムを用いる。「膨大な」暗号化／復号化システムのためにシークレット鍵暗号化システムを用いること（例えば、多数の鍵および多数のパスを用いるDES実現形態である、Skipjack、RC2あるいはRC4など）によって、大量の情報を暗号化し、復号化する際の効率がよくなり、PK能力をもたないPPE 650が、多種多様なアプリケーションでVDEオブジェクト300を処理できるようになる。通信にPK暗号化システムを用いることにより、通信を成立させるのに秘密の共有される外部通信鍵に頼る必要性がなくなり、PPE 650を認証するのに共有される内部秘密に依存しないチャレンジ／レスポンスを実現することができ、共有されるシークレット鍵に依存しなくても公衆が利用可能な証明処理を実現することができるといった、さまざまな利点が得られる。

内容プロバイダの中には、その内容の使用をPK実現形態に限定したいと望む者もいる。このような要望は、例えば、REGISTERメソッドでこのようなオブジェクトに必要とされるものを、登録の継続を許可する前にPPE 650の具体的な、あるいは一般的なPK能力について調べるロードモジュールのかたちで設けることにより、PPE 650でのPK能力の利用可能性とPK能力の具体的な性格またはタイプとをVDEオブジェクト300登録の際の１ファクタとすることによっ

てサポートされうる。

VDE100は、何ら特定のアルゴリズムを要求するわけではないが、すべてのPPE 650が、同一のアルゴリズムを膨大な暗号化／復号化に用いることができることは、非常に望ましい。もし、VDEオブジェクト300を暗号化するのに用いられる膨大な暗号化／復号化アルゴリズムが標準化されないのなら、すべてのVDE電子器具600がすべてのVDEオブジェクト300を操作できるわけではないこともありうる。もし標準化された膨大な暗号化／復号化アルゴリズムの全部または一部が、ハードウェアベースの暗号化／復号化エンジン522により実施されず、その代わりソフトウェアのかたちで実施されるのなら、異なる複数のPPE 650およびそれに

付随する電子器具600の間にパフォーマンスの差が存在することになる。暗号化／復号化エンジン522によりその全部または一部が実施されないアルゴリズムをサポートするためには、このようなアルゴリズムを実施するコンポーネントアセンブリが、PPE 650に利用可能でなければならない。

Ｂ．鍵の長さ

鍵の長さを長くすれば、安全性を増すことができる。暗号化システムに対する「強行」攻撃は、可能なすべての鍵を試してみることを伴う。鍵が長ければ長いほど、試してみるべき可能な鍵も多くなる。ある鍵の長さでは、現在利用可能な計算資源からすると、強行攻撃者が可能なあらゆる鍵を試してみるには、とても実用的ではない莫大な量の時間が必要になることになる。

好ましい実施の形態により提供されるVDE 100は、鍵について異なる多数の長さに対応可能であり、それらを利用することができる。好ましい実施の形態においてVDE 100により用いられる鍵の長さは、暗号化／復号化に用いられる（１つ以上の）アルゴリズム、望まれる安全性のレベル、およびスループット上の要件により決定される。鍵の長さが長くなると、高速な暗号化／復号化応答時間を保証するためには、一般に、処理能力をさらに向上させることが必要になる。よって、（a）安全性と、（b）処理時間および／または資源との間でのトレードオフがおこなわれる。ハードウェアベースのPPE暗号化／復号化エンジン522

は、ソフトウェアベースの暗号化／復号化よりも高速な処理時間を実現することができるので、一般に、ハードウェアベースのアプローチにより、より長い鍵の使用が可能になる。

好ましい実施の形態では、PK暗号化／復号化用に1024ビットモジュラス（鍵）のRSA暗号化システムを用いてもよい。また、「膨大な」暗号化／復号化用には56ビットのDESを用いてもよい。標準的なDESにより提供される56ビットの鍵は、少なくとも最も敏感なVDE情報については、十分な安全性を提供できるほど長くないこともありうるので、さらなる安全性を実現するためには、多数のパスを用い、多数のDES鍵を用いるマルチプルDES暗号化を用いてもよい。DESは、もし異なる複数の鍵と共に多数のパスを用いるように動作させれば、はるかに安全性の

高いものにすることができる。例えば、２つまたは３つの別々の鍵を用いた３つのパスでは、安全性がずっと高くなる。なぜなら、これにより鍵の長さを効果的に長くすることができるからである。RC2およびRC4（DESの代替手段）は、40ビットの鍵サイズまででではエクスポートされうるが、DESレベルの安全性を実現するだけでも、鍵のサイズは、おそらくずっと長くすることが必要であろう。NSAのSkipjackにより提供される80ビットの鍵長さは、ほとんどのVDE安全性要求に適切でありうる。

コードおよびその他の情報をダイナミックにPPE 650にダウンロードする能力により、莫大な数のVDE電子器具600が用いられた後でも、鍵の長さを調整し、ダイナミックに変更することが可能になる。VDE管理者が、それぞれのPPE 650と効率よく通信する能力をもっていれば、このような事後的なダイナミックな変更が可能になり、しかもコスト的にも有効にすることができる。新しい、つまり改良された暗号化システムを現存するPPE 650へとダウンロードすることによって、PPE内で利用可能な暗号化システムのレパートリーを取り替えたり、これに追加することが可能になり、旧式PPEが、新型PPEおよび／または新発売のVDEオブジェクト300およびその他のVDEにより保護された情報と互換性を保つことが可能になる。例えば、異なる鍵の長さ能力を提供することによって、暗号化／復号化エンジン522のハードウェアベースの機能性を補

強するためには、ソフトウェア暗号化／復号化アルゴリズムをいつでもPPE 650にダウンロードすることができる。柔軟性の向上を実現するためには、PPE暗号化／復号化エンジン522は、多数のパス、および／または可変および／またはより長い鍵の長さを予想できるように構成されてもよい。加えて、より長いPK鍵を内部で発生する能力をPPE 650に提供するのも望ましい。

Ｃ．鍵の発生

好ましい実施の形態により提供される鍵発生技術により、PPE 650は、自らにのみ「わかっている」鍵およびその他の情報を発生することができる。

暗号化された情報の安全性は、それを暗号化するのに用いられた鍵の安全性に存する。もし暗号化的には弱い処理を鍵の発生に用いれば、安全性全体が弱くな

る。良好な鍵は、鍵空間における可能なあらゆる鍵が等しい可能性を有している（equally likely）ような、ランダムなビットストリングである。よって、鍵は一般に、例えば、高信頼ランダムソースからシードされた暗号化的に安全な疑似乱数発生器により、そのようなソースから導き出されるべきである。このような鍵発生器は、例えば、Schneierの Applied Cryptography (John Wiley and Sons、1994)、第15頁に記載されている。もし鍵がある与えられたPPE 650の外側で（例えば、別のPPE 650により）発生されたのなら、それらの鍵は、使用される前に高信頼ソースから得られたことを確かめるために検証されなければならない。鍵を検証するためには、「証明」を用いればよい。

好ましい実施の形態によるPPE 650は、鍵の自動的な発生も実現する。例えば、好ましい実施の形態によるPPE 650は、PKベースの外部通信を保護するのに用いられ、その他の理由でも用いられる、それ固有の公開／秘密鍵のペアを発生することができる。PPE 650はまた、初期化中、および初期化後に、さまざまな目的で、それ固有の対称鍵を発生することもできる。PPE 650は安全な鍵環境を提供するので、好ましい実施の形態では、ほとんどの鍵発生は、PPE内でおこなわれうる（ただし、PPEが、自らに対する初期ダウンロードメッセージを認証できるようにするために、製造時またはインストレーション時に用いら

れる初期PPE鍵は、可能な例外である）。

良好な鍵発生は、ランダム性に依存する。好ましい実施の形態によるPPE 650は、図９を参照して前述したように、高信頼の乱数を発生するのに必要な特性を有する、ハードウェアベースの乱数発生器542を備えうる。これらの乱数は、ランダムなシードから導出された追加的な鍵値を発生するための、暗号化的に強力な疑似乱数発生器（例えば、出力フィードバックモードで演算されたDES）を「シード」するのに用いられうる。好ましい実施の形態では、乱数発生器542は、「ノイズダイオード」、あるいはその他の物理ベースの乱数値ソース（例えば、放射線崩壊（radioactive decay））から構成されうる。

もしPPE 650において、利用可能な乱数発生器542がないのなら、SPE 503は、SPE内部で保護された秘密値から導き出された疑似乱数値系列を発生するために、

暗号化アルゴリズム（例えば、出力フィードバックモードでのDES）を用いることができる。これらの数は、真の乱数でなく、疑似乱数ではあるものの、SPE 503外部の未知の値から暗号化的に導き出されるので、ある種のアプリケーションでは十分満足のいくものでありうる。

SPE 503なしにHPE 655を取り入れる実施の形態では、乱数値発生器565のソフトウェアは、予測できない外部物理事象（ディスクI/O完了、または取り付けられたキーボード612のユーザキーストロークの高分解能タイミング）から信頼性の高い乱数を導出することができる。

このような「シード」に基づいてPK鍵および非PK鍵を発生するには、従来の技術を用いればよい。よって、もしパフォーマンスおよび製造コストが許すのなら、PPE 650は、好ましい実施の形態では、それ固有の公開／秘密鍵のペアを、このような乱数または疑似乱数「シード」値に基づいて発生する。この鍵のペアは、その後、その鍵のペアを発生したPPE 650と、それと通信することを望んでいるその他のPPEとの間での外部通信に用いられうる。例えば、発生用PPE 650が、この鍵のペアの公開鍵を他のPPEに漏らすこともありうる。これにより、公開鍵を用いるその他のPPE 650が、発生用PPEのみにより復号化可能なメッセージを暗号化することが可能になる（発生用PPEは、対応する「秘密鍵」を「知っている」唯一のPPEである）。同様に、発生用PPE 650は、その秘密鍵を用いてメッセージを暗号化することもできる。この秘密鍵は、その他のPPEが発生用PPEの公開鍵を用いて復号化に成功すると、発生用PPEがメッセージを送ったことを、その他のPPEが認証できるようにする。

あるPPE 650が、別のPPEにより発生された公開鍵を用いる前に、その公開鍵に対して認証証明書を発行するために、公開鍵証明処理が用いられるべきである。公開鍵の証明書は、例えば認証済みのPPE 650またはVDE管理者のような信頼のおけるエンティティにより「署名された」誰かの公開鍵である。証明書は、実際にはそうではない（例えば、実際には、PPE 650の安全性を破壊しようと企てている人物と通信している）のに、認証済みのPPEと通信しているとPPE 650を言いくるめようとする企てを妨害するのに用いられる。好ましい実施の形態では、１つ

以上のVDE管理者が、証明機関を構成しうる。PPE 650により発生された公開鍵と、PPEおよび／または対応するVDE電子器具600に関する情報（例えば、サイトID、ユーザID、失効日、名前、アドレスなど）との両方に「署名する」ことによって、VDE管理者証明機関は、PPEおよび／またはVDE電子器具に関する情報が正しいこと、およびその公開鍵が特定のVDEモードに属することを証明できる。

証明書は、ディジタル署名の信頼度については重要な役割を果たす。また、公開鍵認証通信プロトコル（後述する）においても重要である。好ましい実施の形態では、これらの証明書は、ある特定のVDE電子器具600の信頼度／安全性レベルに関する情報（例えば、ハードウェアベースのSPE 503をもっているかどうか、あるいは信頼度の劣るソフトウェアエミュレーションタイプのHPE 655を代わりにもっているのか）を含んでいてもよい。この情報は、非常に安全性の高い情報を信頼度／安全性の劣るVDEインストレーションに送信するのを避けるのに用いられうる。

証明書は、非委託型の悪質（decommissioning rogue）ユーザおよび／またはサイトにおいても重要な役割を果たしうる。サイトおよび／またはユーザIDを証明書に含ませることによって、PPEは、この情報を認証の一局面として評価

することができる。例えば、もしVDE管理者または情報交換所が、ある種の（例えば、非委託型および／またはさもなくば疑わしいユーザおよび／またはサイトのリストに載っているような）基準を満たしているID（またはその他の情報）をもつ証明書に遭遇すれば、これらの基準に基づいて、通信の拒否、ディセーブル情報の通信、ユーザへの状況の通知といったいくつかのアクションのいずれかを選択することができる。また、証明書は、典型的には、例えば、サイトおよび／またはユーザはVDE管理者と常にコンタクトをとっていなければならないことを確認し、および／または証明鍵を定期的に変更可能とするため、証明書は定期的に書き換えられなければならないことを確認するための失効日を含んでいる。たとえある与えられた証明鍵が侵犯されても、１つ以上の「バックアップ」証明書を用いることができるように、異なる複数の鍵に基づく１つよりも多くの証明書を、サイトおよび／またはユーザに対して発行することができる。もしある証明

鍵が侵犯されれば、VDE管理者は、このような鍵を用いて発行された証明書に基づいて認証するのを拒否し、さらに続くVDE加入者とのインタラクションにおいて、侵犯された鍵のすべての使用と、その鍵に関わるあらゆる証明書とを無効にする「バックアップ」証明書を用いて認証した後、信号を送ることができる。新しい１つ以上の「バックアップ」証明書および鍵は、このような侵犯の後、認証されたサイト／ユーザに対して作成され、送られうる。

もし多数の証明書を利用可能であるのなら、それらの証明書中のいくつかをバックアップとしてとっておくことができる。あるいは、またはそれに加えて、一群の証明書の中からある証明書をある与えられた認証で（例えば、RSG 542を用いて）選択することによって、侵犯された証明鍵に関連する証明書が用いられる可能性を低くすることができる。さらに、ある与えられた認証で１つよりも多くの証明書を用いてもよい。

証明アルゴリズムが（例えば、このアルゴリズムの元になっている数学的基礎の予測不可能な進歩により）侵犯される可能性に対して防衛策を講じるためには、異なる複数の数学的基礎に基づく異なる複数の証明書に、別々のアルゴリズムを用いてもよい。

侵犯される可能性を低下させるのに用いられうる別の技術としては、それらの証明書の元になっている「公開」値を（PPE 650の保護された記憶装置で）秘密のままにしておくことによって、攻撃の助けになるような値への攻撃者のアクセスを拒否するやりかたがある。これらの値は、名目上は「公開」であるものの、それらの値は、実際に証明書の有効性を検査するこれらの構成員（つまり、PPE 650）のみに知らせておく必要がある。

好ましい実施の形態では、PPE 650がそれ固有の証明書を発行してもよいし、あるいは、この証明書は、外部から（例えば、証明機関であるVDE管理者などから）得られるようにしてもよい。このディジタル証明書がどこで発行されたかには関わりなく、その証明書は、最終的には、他のVDE電子器具600がこの公開鍵にアクセスする（かつそれを信頼する）ことができるように、VDE管理者証明機関により登録される。例えば、PPE 650は、その公開鍵およびその他の情報を証明

機関へと通信することができる。これに応答して、証明機関は、証明機関の秘密鍵を用いて、その公開鍵およびその他の情報を暗号化する。その他のインストレーション600は、この「証明書」を信頼することができる。なぜなら、この証明書は、その復号化に証明機関の公開鍵を用いて認証されるからである。別の例としては、証明機関は、発生用PPE 650から受け取った公開鍵を暗号化し、かつ証明機関の秘密鍵を暗号化にこの公開鍵を用いることができる。その後、証明機関は、この暗号化された情報を発生用PPE 650に送り返すことができる。発生用PPE 650は、その後、内部でディジタル証明書を作成するのに、証明機関の秘密鍵を用いることができる。その後、発生用PPE 650は、証明機関の秘密鍵のコピーを破壊することができる。発生用PPE 650は、次に、もし望みとあれば、ディジタル証明書を送り出して、VDE管理者（あるいは他のどこでもよいが）にある証明格納場所に格納されるようにする。この証明処理は、また、外部鍵ペア発生器および証明書発行器を用いて実施することもできるが、安全設備の性格によっては、安全性がいくらか劣ることもある。そのような場合、PPE 650では、関連するその他の鍵に曝される程度を制約するために、製造鍵が用いられるべきである。

PPE 650は、１つよりも多くの証明書を必要とすることもある。例えば、PPEが認証済みであることを他のユーザに確認させ、かつそのPPEを識別するために、証明書が必要なこともある。さらにいくつかの証明書が、PPE 650の個々のユーザに必要になることもある。これらの証明書は、ユーザおよびサイト両者の情報を取り入れることもできるし、ユーザの情報のみを含ませることもできる。一般に、証明機関は、ある与えられたユーザに対して証明書を作成する以前に、有効なサイト証明書の提示を要求するものである。ユーザはそれぞれ、証明書を得るためには、自らの公開鍵／秘密鍵ペアを必要とする。VDE管理者、情報交換所、およびその他の加入者は、通常、通信している、または他のかたちでインタラクションしているサイト（PPE 650）およびユーザの両方について認証を要求することができる。鍵の発生およびPPE 650への証明に関する上記処理は、サイト／ユーザ証明書あるいはユーザ証明書をつくるのに用いられてもよい。

上述した証明書は、ロードモジュール1100の源（origin）および／または管理

操作の認証性（authenticity）を証明するのに用いられてもよい。上述した安全性および保証技術は、このような証明書（VDE電子器具600のアイデンティティ証明書以外の証明書を含む）のどれでも、それが侵犯される可能性を低くするのに用いられうる。

Ｄ．鍵の老化と旋回

PPE 650もまた、好ましい実施の形態では、シークレット鍵と、多数のPPE 650の間で共有されるその他の情報とを発生する能力を有している。好ましい実施の形態では、このようなシークレット鍵およびその他の情報は、共有される秘密情報が電子器具間で明示的に通信されることを少しも必要とせずに、多数のVDE電子器具600間で共有されうる。もっと具体的にいえば、PPE 650は、多数のVDE電子器具600間で共有されるシード情報に応答し、決定論的処理に基づいて鍵を導き出すための、いわゆる「鍵旋回（key convolution）」技術を用いる。多数の電子器具600は、その「シード」情報が何であるかを「知ってお

り」、しかもこの情報に基づいて鍵を発生するのに用いられる決定論的処理も「知っている」ので、これらの電子器具はそれぞれ、「真の鍵」を独立して発生することができる。これにより、共通のシークレット鍵を安全ではないチャネル上で通信することで、その安全性が侵犯される可能性もなく、多数のVDE電子器具600が、同一の共通シークレット鍵を共有することができる。

暗号化鍵は、はっきりと決められていない期間のあいだ用いられるべきではない。鍵が用いられる期間が長くなればなるほど、それが侵犯される可能性も高くなり、もしその鍵が侵犯されているのに、それでも新しい情報を保護するのに用いられているのなら、それが失われる可能性も高くなる。また、鍵が用いられる期間が長くなればなるほど、その鍵はより多くの情報を保護することになるので、誰かがそれを破壊するのに必要な努力を払ったとすれば、それにより得られる可能性のある報酬もそれだけ高くなる。さらには、鍵が用いられる期間が長くなればなるほど、暗号文ベースの攻撃を用いて、その鍵を破壊しようと企てている攻撃者が入手可能な暗号文の量もそれだけ増えることになる。Schneierの第150～151頁を参照のこと。鍵の旋回は、好ましい実施の形態では、周期的なルーチ

ンまたはその他の基準に基づき、鍵の変更に伴う周辺の鍵管理問題を簡単にしつつ、安全データベース610に格納されている鍵を効率よく変更するためのメソッドを提供する。加えて、鍵の旋回は、鍵の使用および／または有効性について「失効日」を設けるための「時間老化した鍵」（後述する）を実現するのにも用いられうる。

図62は、好ましい実施の形態における鍵旋回の一実現形態例を示している。鍵の旋回は、サイトID 2821と、RTC 528の上位ビットとの組み合わせを用いることによって、大きな尺度（例えば、1時間または1日単位）で時間依存のサイト固有値である「V」を生じるようにおこなわれうる。この値「V」は、旋回シード値2861を「現在の旋回鍵」2862に変換する暗号化処理2871用の鍵として用いられうる。シード値2861は、ユニバーサルである範囲、またはグループの範囲で共有される秘密値でありうる。また、この値は、安全鍵記憶装置（例えば、PPE 650内の保護されたメモリ）内に格納されうる。シード値2861は、製

造処理中にインストールされ、VDE管理者により随時更新されうる。異なる複数セットのオブジェクト300に対応する複数のシード値2861があってもよい。

現在の旋回鍵2862は、サイトID 2821および現在の時刻の符号化を表す。この変換された値2862は、オブジェクトのPERC 808に格納されている鍵810を、そのオブジェクトの内容に合わせた真の秘密本文鍵（private body key）2863に変換する別の暗号化処理2872用の鍵として用いられうる。

ブロック2861、2871によりおこなわれる「旋回関数」は、例えば、内容作成者のサイトおよび内容ユーザのサイトの両方において独立しておこなわれうる一方向関数でありうる。もし内容ユーザが、内容作成者の用いたものと正確に同じ旋回関数および正確に同じ入力値（例えば、時刻および／またはサイトおよび／またはその他の情報）を用いないのなら、内容ユーザによりおこなわれる旋回関数の結果は、内容作成者の結果とは違ってくることもある。もしその結果が、内容作成者により暗号化のための対称鍵として用いられるのなら、内容ユーザは、内容ユーザの結果が内容作成者の結果と同じでない限り、復号化はできなくなる。

鍵旋回関数への入力の時間成分は、RTC 528から導出されうる（なお、VDE電子

器具間のRTC同期におけるわずかな差によって、異なる複数の電子器具が異なる複数の時間成分を用いることにならないことが確実になるように注意されたい）。RTC 528出力の異なる部分は、複数の鍵に異なる複数の有効持続時間を与えるのに用いられうる。あるいは、処理中で、いくつか異なる鍵値を試してみるためにある程度の許容誤差を導入してもよい。例えば、時間許容誤差を日、週あるいはその他の期間を単位として設けるように、「時間細分性（granularity）」パラメータを調整することができる。一例としては、もし「時間細分性」が２日に設定され、許容誤差が±２日であるのなら、３つのリアルタイム入力値が、旋回アルゴリズムへの入力として試されうる。結果として得られる鍵値はそれぞれ、可能な複数の鍵のうちのどれが実際に用いられているかを決定するために試されうる。この例では、これらの鍵は、わずか４日の寿命しかないことになる。

図63は、ユーザのRTC 528と作成者のRTC 528との間のスキュー（skew）を補償するために、適切に旋回された鍵がどのようにして取り上げられるかを示

している。旋回鍵2862（a～e）のシーケンスは、異なる複数の入力値2881（a～e）を用いることによって発生されうる。これらの入力値はそれぞれ、サイトID 2821およびRTC 528の値±差分値（例えば、-2日、-1日、Δなし、+1日、+2日）として導出される。旋回ステップ2871（a～e）は、鍵2862（a～e）のシーケンスを発生するのに用いられる。

一方、作成者のサイトは、自らのRTC 528の値（鍵の意図された有効期間（validity time）に対応するように調整されている）に基づき、旋回ステップ2871（z）を用いることによって、旋回された鍵2862（z）を発生することができる。この鍵は、その後、オブジェクトのPERC 808で内容鍵2863を発生するのに用いられうる。オブジェクトの内容を復号化するために、ユーザサイトは、その旋回鍵2862（a～e）のシーケンスのそれぞれを用いることによって、親内容鍵810を発生しようと試みる。これが試みられる時、作成者サイトのRTC 538がユーザサイトのRTC 528と比べて許容可能な誤差範囲内にある限り、鍵2862（a～e）の１つが鍵2862（z）と一致し、復号化に成功することになる。この例では、一致しているかどうかは、鍵同士の直接の比較によってではなく、復号化された出力の有効

性によって判定される。

上述した鍵旋回は、必ずしもサイトIDおよび時刻の両方を一つの値として用いる必要はない。いくかの鍵は、現在のリアルタイムに基づいて発生されてもよい。他の鍵は、サイトIDに基づいて発生されてもよい。さらに他の鍵は、現在のリアルタイムおよびサイトIDの両方に基づいて発生されてもよい。

鍵の旋回は、「時間老化した」鍵を設けるために用いられてもよい。これらの「時間老化した」鍵は、鍵を失効させ、「新しい」鍵に取り替えられるようにする自動的メカニズムを提供する。これらの鍵は、ユーザに再登録を要求することなく、また、内容プロバイダや管理者の手に大きな制御権を委ねたままにしておくことなく、１個のオブジェクトの全部または一部について、ユーザに時間の限定された使用を許可する時間の限定された権利を与えるためのメソッドを提供する。もし安全データベース610が十分に安全であるのなら、同様の能力は、鍵に関連づけられた失効日／時刻をチェックすることによっても実現されうる。しかし、これにより、それぞれの鍵または鍵のそれぞれのグループについてより大きな記憶空間を用いることが必要になる。

好ましい実施の形態では、PERC 808は、失効日および／または失効時刻を含むことができる。この失効日／時刻の後、それらに対応するVDEにより保護された情報へのアクセスは、もはや承認されない。あるいは、またはこれに加えて、電子器具600あるいは１つ以上のVDEオブジェクト300の使用のある局面に関わる持続時間の後、PERC 808は、（１つ以上の）オブジェクトを使用する権利を再び得る、または保持するために、監査履歴情報を情報交換所、配付者、クライアント管理者あるいはオブジェクト作成者に送ることをユーザに強制することができる。PERC 808は、鍵の使用および／または承認された使用の過去の利用可能時間を限定するパラメータをチェックする／強要することによって、このような時間ベースの制約を強要することができる。「時間老化した」鍵は、このタイプの時間に関連するアクセス制御をVDEにより保護された情報に強要したり、強化するのに用いられうる。

「時間老化した」鍵は、ある限定された期間のあいだに、１セットの情報を暗

号化／復号化するのに用いられうる。よって、再登録、または新しいパーミッションの受け取り、あるいは監査情報の受け渡しが必要になる。そうしなければ、新しい鍵が提供されてユーザが使用できるようにはならない。時間老化した鍵は、また、システムの安全性を改善するためにも用いられうる。なぜなら、１つ以上の鍵が、時間老化基準に基づいて自動的に取り替えられるからである。よって、安全データベース610を破壊して(cracking)、１つ以上の鍵の位置を突き止めても、本当の値がないことになりうる。時間老化した鍵を用いることにより得られるさらに別の利点としては、それらの鍵がダイナミックに発生されうるということである。これにより、復号化鍵を２次的なおよび／または安全なメモリに格納する必要がなくなる。

「時間老化した」鍵は、好ましい実施の形態では、暗号化／復号化に用いられうる「真の鍵」ではなく、PPE 650が、その他の情報を参照して、「真の鍵」を発生するのに用いることができる情報の断片である。この他の情報は、時間ベースであるか、PPE 650の特定の「ID」に基づくものであるか、あるいはこれらの両者に基づくものでありうる。「真の鍵」は決して曝されることはなく、常に安全なPPE 650環境内で発生されるものであり、また安全なPPEには、「真の鍵」を発生することが要求されるので、VDE 100は、「時間老化した」鍵を、システムの安全性および柔軟性の大幅な強化に用いることができる。

鍵を「老化させる」処理は、好ましい実施の形態では、(a)「真の鍵」および(b)その他の何らかの情報（例えば、リアルタイムパラメータ、サイトIDパラメータなど）の関数である時間老化した「真の鍵」を発生することを必然的に伴う。この情報は、「真の鍵」を復元するか、または提供するために、（例えば、上述した「鍵の旋回」技術を用いて）組みあわされ／変換される。「真の鍵」は復元されうるので、これにより、「真の鍵」をPERC 808内に格納することを避けることができ、かつ異なる複数の「真の鍵」が、PERC 808内の同一の情報に対応するようにすることができる。「真の鍵」は、PERC 808には格納されないので、PERCにアクセスしても、「真の鍵」により保護されている情報へのアクセスが可能になることはない。よって、「時間老化した」鍵は、内容作成者／プロバイ

ダが情報のアクセスに（例えば、サイトベースのおよび／または時間ベースの）制約を課すことを可能にする。情報へのアクセスは、ある意味では、１つ以上のPERC 808により提供されるパーミッションの「外部」にあるか、あるいはそれを補助するものである。例えば、「時間老化した」鍵は、ある種の保護された情報へのアクセスに追加の時間制限を強要することができる。この追加の時間制限は、PERC 808内に含まれるどの情報あるいはパーミッションからも独立しているが、その代わり１つ以上の時間および／またはサイトID値に基づくものである。

一例として、時間老化した暗号化鍵は、電子的に出版された新聞を「暫定予約購読」のかたちで購入する者が、一週間のあいだ、この新聞のそれぞれの版にアクセスできるようにするために用いられうる。一週間の経過後、暗号化鍵は、もはや機能しなくなる。この例では、ユーザが、その一週間の間に得られた版以外の版にアクセスするには、１つ以上の新しいPERC 808を購入したり、現存する１つ以上のパーミッション記録への更新を受け取ったりする必要がある。これらその他の版へのアクセスは、全く別の価格決定構造（例えば、無料あるいは最少額の「暫定」予約購読レートとは対照的な「通常の」予約購読レート）を用いても操作されうる。

好ましい実施の形態では、時間老化ベースの「真の鍵」は、一方向の、または可逆的な「鍵旋回」関数を用いて発生されうる。旋回関数への入力パラメータは、供給された時間老化した鍵と、ユーザおよび／またはサイト特異値と、RTC 528からの時間値の指定された部分（例えば、ある数の上位ビット）あるいは所定の手法によりこのような時間値から導き出された値と、時間老化した鍵がユニークなものであることを確かめるのに用いられうるブロックあるいはレコード識別子とを含みうる。「鍵旋回」関数の出力は、破棄されるまで復号化を目的として用いられる「真の鍵」でありうる。時間老化した鍵と、適切ではない時間値とを用いてこの関数をランしても、典型的には、復号化できない無用な鍵が生じるだけである。

新しい時間老化した鍵の発生は、経過した絶対時間あるいは相対時間のある値に基づいて（例えば、RTC 528のようなクロックからのリアルタイム値に基づい

て）トリガされうる。その時、旋回は、間違った鍵を生成する。また、復号化は、時間老化した鍵が更新されるまで、おこなわれない。いつ新しい「時間老化した鍵」が作成されるべきであるかを決定するのに用いられる基準は、さらに別の安全性レベルを実現するために、時間あるいはその他の入力変数に基づいて、それ自体が変更されてもよい。よって、旋回関数および／またはそれを実施するイベントは、可変量をパラメータとして変更したり、シフトさせたり、用いたりすることができる。

時間老化した鍵の使用例としては、以下のものがある。

１）作成者が、「真の鍵」を作成し、それを用いて内容を暗号化する。

２）作成者が、「逆旋回」への入力パラメータとして

ａ）「真の」鍵、

ｂ）時間パラメータ（例えば、RTC 528の有効な上位時間ビット）および

ｃ）その他のオプションの情報（例えば、サイトIDおよび／またはユーザID）

を用いて「時間老化した鍵」を生じるために、「逆旋回」をおこなう。

３）作成者が、「時間老化した」鍵を内容ユーザに配付する（作成者は、もし内容ユーザのPPE 650に既に利用可能な旋回アルゴリズムを用いていないのなら、旋回アルゴリズムおよび／またはパラメータをも配付する必要がある）。

４）内容ユーザのPPE 650が、

ａ）「時間老化した」鍵、

ｂ）上位時間ビット、および

ｃ）要求されたその他の情報（2cと同）

を組みあわせる。

内容ユーザのPPE 650は、「真の」鍵を得るために、旋回関数（つまり、上記ステップ（2）の「逆旋回」アルゴリズムの逆）をおこなう。もし供給された時間および／またはその他の情報が「間違っている」のなら、旋回関数は、「真の」鍵を生成しないので、内容は復号化されえない。

VDEオブジェクト300あるいはその他のアイテムに関連づけられた鍵ブロックは

いずれも、オブジェクトコンフィギュレーション処理の間にオブジェクト作成者により指定されたとおりに、あるいはそれが適切な場合には、配付者またはクライアント管理者により指定されたとおりに、通常の鍵ブロックあるいは時間老化した鍵ブロックのいずれかでありうる。

「時間老化した」鍵は、また、PPE 650間の安全な通信を実現するためのプロトコルの一部としても用いられうる。例えば、「真の」鍵を通信用のPPE 650に提供する代わりに、VDE 100は、「部分的な」通信鍵のみをPPEに供給することもできる。これらの「部分的な」鍵は、例えば初期化のあいだにPPE 650に供給されうる。所定のアルゴリズムによって、安全な通信のために情報を暗号化／復号化するのに用いられる「真の鍵」を生成することができる。この所定のアルゴリズムは、すべてのPPE 650でこれらの鍵を同じように「老化させる」ことができる。あるいはPPE 650には、部分通信鍵の新しいセットがPPEへと

ダウンロードされうるように、ある所定の時刻にVDE管理者とコンタクトをとることが要求されることもある。もしPPE 650が「新しい」部分鍵を発生しないか、さもなくば得ないのなら、PPE 650は、その他のPPEとの通信についてディセーブルされる（PPEが、再初期化を目的としてVDE管理者と確実に通信できるように、別の「フェールセーフ（fail safe）」鍵が提供されてもよい）。２セットの部分鍵をPPE 650内に維持することによって、すべてのVDE器具600間で固定された量のオーバーラップ時間を実現することができる。これら２セットの部分鍵のうち古いほうのセットは、周期的に更新されうる。

好ましい実施の形態では、以下の追加タイプの鍵（後述する）も、「老化」されうる。

個々のメッセージ鍵（すなわち、特定のメッセージに用いられる鍵）、

管理用の、静止および移動オブジェクト共有鍵、

安全データベース鍵、および

秘密本文鍵および秘密内容鍵

初期インストレーション鍵管理

図64は、PPE 650を生成する間のユニバーサル範囲の、すなわち「親」鍵のフ

ローを示している。好ましい実施の形態では、PPE 650は、製造者およびPPE自身によって発生された鍵を用いて初期化される、安全不揮発性鍵記憶装置2802（例えば、SPU 500の不揮発性RAM 534BまたはHPE 655により保守される保護された記憶装置）を含んでいる。

製造者は、サイト識別証明書2821に署名したり、それの有効性を検査するのに用いられる１つ以上の公開鍵2811／秘密鍵2812の鍵ペアを保有している（すなわち、それを知っており、開示または改変からそれを保護する）。それぞれのサイトについて、製造者は、サイトID 2821およびサイト特性リスト2822を発生する。加えて、製造者は、ロードモジュールおよび初期化コードダウンロードの有効性を検査するための公開鍵2813、2814をも保有している。安全性を強化するために、このような証明鍵は複数個あってもよいし、それぞれのPPE

650が、それぞれのタイプのこのような鍵のうち１サブセットのみを用いて初期化されてもよい。

初期化処理の一部として、PPE 650は、１ペア以上のサイト特異的な公開鍵2815および秘密鍵2816を内部で発生してもよいし、あるいは製造者がそれを発生して供給してもよい。これらは、PPE 650により、そのアイデンティティを証明するために用いられる。同様に、そのサイトに対する（１つ以上の）サイト特異的なデータベース鍵2817が発生される。もし必要なら（つまり、もし乱数発生器542が利用可能ではないのなら）、乱数初期化シード2818が発生される。

初期化は、サイトのID 2821および特性2822ならびにサイトの公開鍵2815／秘密鍵2816のペア（１つ以上）を発生することにより始まってもよい。これらの値は組み合わされ、１つ以上のサイトアイデンティティ証明書2823を発生するのに用いられうる。サイトアイデンティティ証明書2823は、公開鍵発生処理2804により発生されうるし、PPEの保護された鍵記憶装置2802および製造者のVDEサイト証明書データベース2803の両方に格納されうる。

証明処理2804は、製造者によっても、あるいはPPE 650の内部でもおこなわれうる。もしPPE 650によりおこなわれるのなら、PPEは、アイデンティティ証明秘密鍵2812を一時的に受け取り、証明書2823を発行し、その証明書を局所鍵記憶装

置2802に格納した後、それを製造者に伝送する。その後、PPE 650は、アイデンティティ証明秘密鍵2812のコピーを消去しなければならない。

引き続いて、初期化は、PPE 650あるいは製造者による、（１つ以上の）サイト特異的なデータベース鍵2817および（１つ以上の）サイト特異的なシード値2818の発生を要求しうる。これらは、鍵記憶装置2802に格納される。加えて、（１つ以上の）ダウンロード証明鍵2814およびロードモジュール証明鍵2813が、製造者により供給されて、鍵記憶装置2802に格納されうる。これらは、PPE 650により、外部エンティティとのさらなる通信のすべての有効性を検査するために用いられうる。

この時点において、PPE 650は、（１つ以上の）ロードモジュール鍵2813および（１つ以上の）ダウンロード鍵2814により証明された情報をダウンロードすることによって、実行可能なコードおよびデータを用いてさらに初期化されうる。好ましい実施の形態では、これらの鍵は、その有効性を保証するPPE 650にロードされるデータにディジタル的に署名するのに用いられる。また、（１つ以上の）サイト特異的な公開鍵2815を用いて暗号化された（１つ以上の）追加の鍵は、このようなデータを暗号化し、それを開示から保護するのに用いられうる。

インストレーションおよび更新鍵管理

図65は、製造者、またはVDE管理者による後続更新のいずれかによるさらなる鍵インストレーションの例を示している。製造者または管理者は、（１つ以上の）秘密ヘッダ鍵2831、（１つ以上の）外部通信鍵2832、管理オブジェクト鍵2833あるいはその他の（１つ以上の）共有鍵2834に対する初期値または新しい値を供給することができる。これらの鍵は、グローバル証明鍵2811、2813および2814と同じ意味合いでユニバーサル範囲でありうる。あるいは、これらの鍵は、VDE事例のある規定されたグループ内での使用に限定されてもよい。

このインストレーションをおこなうために、インストーラは、デスティネーションサイトの（１つ以上の）アイデンティティ証明書2823を取り出し、そこから（１つ以上の）サイトの公開鍵2815を抽出する。これら（１つ以上の）鍵は、暗号化処理2841において、インストールされている鍵を保護するのに用いられうる

。インストールされているこれら（１つ以上の）鍵は、その後、デスティネーションサイトのPPE 650内部で伝送される。PPE 650の内部では、復号化処理2842は、伝送を復号化するために、（１つ以上の）サイトの秘密鍵2816を用いることができる。その後、PPE 650は、インストールされたあるいは更新された鍵を鍵記憶装置2802に格納する。

オブジェクト固有の鍵の使用

図66および図67は、VDEオブジェクト300に関連づけられたデータおよび制御情報を保護する際の鍵の使用を示している。

図66は、静止内容オブジェクト850を示している。その制御情報は、管理オブジェクト870から導き出される。これらのオブジェクトは、PPE 650により受け取られうる（例えば、ネットワークを介してオブジェクト格納場所728から取り出されたり、ローカル記憶装置から取り出されたりする）。管理オブジェクト復号化処理2843は、（１つ以上の）秘密ヘッダ鍵2815を用いて管理オブジェクト870を復号化することによって、内容オブジェクト850へのアクセスを支配するPERC 808を取り出すことができる。その後、（１つ以上の）秘密本文鍵810が、PERC 808から抽出され、その内容をPPE 650外部でも利用できるように内容復号化処理2845により用いられる。加えて、（１つ以上の）データベース鍵2817が、PPE 650外部の安全データベース610にPERCを格納する準備のため暗号化処理2844により用いられる。内容オブジェクト850へと後にアクセスする時には、PERC 808は、安全データベース610から取り出され、（１つ以上の）データベース鍵2817を用いて復号化された後、管理オブジェクト870から抽出されるのではなく、直接、使用される。

図67は、移動オブジェクト860を伴う同様の処理を示している。図66と図67との間の主な違いは、PERC 808が移動オブジェクト860の中に直接、格納されることであり、よって、（１つ以上の）秘密ヘッダ鍵2831を提供するために、復号化処理2843の直後に用いられうることである。この秘密ヘッダ鍵2831は、移動オブジェクト860内の内容を処理するのに用いられる。

シークレット鍵の変化

図64～図67は、好ましい公開鍵の実施の形態を示しているが、シークレット鍵バージョンを理解する一助としても用いられうる。シークレット鍵の実施の形態では、証明処理および公開鍵暗号化／復号化の代わりに、秘密鍵暗号化がおこなわれ、公開鍵／秘密鍵ペアの代わりに、PPE 650の事例とその他のパーティ（例えば、（1つ以上の）ロードモジュール供給者、PPE製造者など）との間で共有される個々のシークレット鍵が用いられる。加えて、証明処理2804は、シークレット鍵による実施の形態ではおこなわれず、サイトアイデンティティ証明書2823もVDE証明書データベース2803も存在しない。

鍵のタイプ

以下に述べる鍵のタイプの詳細な説明では、シークレット鍵の実施の形態をさらに説明している。しかし、この要旨は、完全な記述を意図しているわけではない。好ましい実施の形態によるPPE 650は、異なる複数のタイプの鍵および／または異なる複数の「共有される秘密」を異なるさまざまな目的で用いることができる。いくつかの鍵タイプは、公開鍵／シークレット鍵の実現形態に適用され、他の鍵は、シークレット鍵の実現形態のみに適用され、さらに他の鍵タイプは、それらの両者に適用される。以下の表は、好ましい実施の形態において用いられるさまざまな鍵および「共有される秘密」情報の例をリストアップしたものである。この情報は、用いられ、格納される場所もリストアップしている。

鍵／秘密情報のタイプ	PK または非 PK のどちらで用いるか	（１つ以上の）格納位置の例
（１つ以上の）親鍵（後述する具体的な鍵のいくつかを含みうる）	両方	PPE 製造設備 VDE 管理者
製造鍵	両方（望みとあればPK）	PPE（PK の場合） 製造設備
証明鍵のペア	PK	PPE 証明格納場所
公開／秘密鍵のペア	PK	PPE 証明格納場所（公開鍵のみ）
初期シークレット鍵	非 PK	PPE
PPE 製造 ID	非 PK	PPE
サイト ID、共有コード、共有鍵および共有秘密	両方	PPE

ダウンロード承認鍵	両方	PPE VDE 管理者
外部通信鍵およびその他の情報	両方	PPE 安全データベース
管理オブジェクト鍵	両方	パーミッションレコード
静止オブジェクト鍵	両方	パーミッションレコード
移動オブジェクト共有鍵	両方	パーミッションレコード
安全データベース鍵	両方	PPE
秘密本文鍵	両方	安全データベース いくつかのオブジェクト
内容鍵	両方	安全データベース いくつかのオブジェクト
承認共有秘密	両方	パーミッションレコード
安全データベースバックアップ鍵	両方	PPE 安全データベース

親 鍵

「親」鍵は、その他の鍵を暗号化するのに用いられる鍵である。初期鍵つまり「親」鍵は、安全なメソッドでその他の鍵と通信するために、PPE 650内に設けることができる。PPE 650の初期化の間、コードと共有鍵とがPPEにダウンロードされる。このコードは、安全旋回アルゴリズムおよび／または係数を含んでいるので、このコードは、「親鍵」に相当する。共有鍵もまた、「親鍵」と見なすことができる。

もし公開鍵暗号化が、PPE 650との外部通信の基礎として用いられるのなら、PPE公開鍵ペアの証明処理の間に親鍵が必要になる。この親鍵は、例えば、ディジタル証明書（暗号化された公開鍵およびPPEのその他の情報）を成立させるために、製造者もしくはVDE管理者により用いられる秘密鍵でありうる。また、この親鍵は、別の例では、証明書格納場所内のエントリを暗号化するために

VDE管理者により用いられる秘密鍵であってもよい。いったん証明がおこなわれれば、PPE 650間の外部通信は、PPEと通信していることの証明書を用いて、成立させることができる。

もし共有シークレット鍵が、外部通信の基礎として用いられるのなら、PPE 650初期化のための外部通信を成立させるためには、初期シークレット鍵が必要になる。この初期シークレット鍵は、その他の鍵を暗号化するのに用いられるという意味合いで、「親鍵」である。PPE初期化処理の間に、共有部分外部通信鍵（上述した）のセットがダウンロードされてもよい。また、これらの鍵は、後続する外部PPE通信を成立させるのに用いられる。

製造鍵

製造鍵は、初期化時にPPEにダウンロードされるPPE固有の鍵情報について製造スタッフが知るのを防止するために、PPEの製造時に用いられる。例えば、製造設備の一部として動作するPPE 650は、初期化されているPPEにダウンロードするための情報を発生することができる。この情報は、PPE 650間の通信のあいだに、その秘匿性を維持するために暗号化されなければならない。そうしなければ、製造スタッフがこの情報を読むことができるからである。製造鍵は、この情報を保護するために用いられる。また、製造鍵は、例えば、証明秘密鍵や、PPEの公

開／秘密鍵ペアや、および／またはPPEに固有の共有シークレット鍵のようなその他の鍵といった、PPEにダウンロードされるその他さまざまな鍵を保護するのに用いられうる。製造鍵は、他の鍵を暗号化するのに用いられるので、これも「親鍵」である。

製造鍵は、公開鍵に基づいていてもよいし、共有の秘密に基づいていてもよい。いったん情報がダウンロードされれば、現在初期化されているPPE 650は、この製造鍵を破棄する（あるいは単に使用しない）ことができる。製造鍵は、製造時にPPE 650へと結線されうるし、PPEへとその最初の鍵として送られ、もはや必要なくなった後で破棄されてもよい。上記テーブルおよび前節の議論で示したように、もしPK能力がPPEに設けられていれば、製造鍵は、必要ではない。

証明鍵のペア

証明鍵のペアは、PPE 650およびVDE電子器具600用の「証明」処理の一部として用いられうる。この証明処理は、好ましい実施の形態では、VDE電子器具が、それ（すなわち、その鍵）が信頼されうることを認証する１つ以上の「証明書」を提示できるようにするのに用いられうる。上述したように、この「証明」処理は、１つのPPE 650により、それが認証済みのVDE PPEであること、一定のレベルの安全性および能力セット（例えば、単なるソフトウェアベースのものではなく、ハードウェアベースのものであること）を有していることなどを「証明する」ために用いられうる。簡単にいうと、「証明」処理は、別のVDEノードの公開鍵を含むメッセージを暗号化するために証明鍵ペアのうち証明書秘密鍵の使用を伴うことがある。証明鍵ペアの秘密鍵は、好ましくは、PPE証明書を発行するのに用いられる。この鍵は、PPEの公開鍵を暗号化するのに用いられる。PPE証明書は、PPEに格納されてもよいし、証明書格納場所に格納されてもよい。

選択された認証技術次第では、証明鍵ペアの公開鍵および秘密鍵は、保護される必要があることもある。好ましい実施の形態では、１つ以上の証明公開鍵が、認証の一局面として証明書を復号化するのに用いることができるように、PPE間に配付される。好ましい実施の形態では、この公開鍵はPPE 650の内部で用いられるので、この公開鍵が、平文で利用可能である必要はない。いずれにせよ、こ

のような鍵が完全性を保ったままで（例えば、VDE管理者による初期化および／または更新の間に）保守され、伝送されるようにすることは重要である。もし証明公開鍵の秘匿性が維持されれば（すなわち、PPE 650内部で平文のかたちでのみ利用可能であるのなら）、その安全性を破壊する（cracking）ことは、ずっと困難になる。証明鍵ペアの秘密鍵は、その秘匿性が維持されるべきであり、また証明機関のみによって格納されるべきである（つまり、配付されるべきではない）。

好ましい実施の形態において、互いに異なるレベル／程度の信頼性／安全性をもつ複数のインストレーションを差別化する能力を可能にするためには、異なる複数の証明鍵ペアを用いればよい（例えば、異なる複数の証明鍵は、SPE 503を証明するために用いられた後、HPE 655を証明するために用いられてもよい）。

ＰＰＥ公開／秘密鍵ペア

好ましい実施の形態では、PPE 650はそれぞれ、それ固有のユニークな「デバイス」（および／またはユーザ）の公開／秘密鍵ペアを有していてもよい。好ましくは、この鍵ペアのうちの秘密鍵は、PPE内で発生され、いかなる形態でもPPEの外部に曝されることは決してない。よって、ある実施の形態では、PPE 650には、鍵のペアを内部で発生する内部能力が設けられてもよい。もしPPEがそれ固有の公開鍵暗号化システムの鍵ペアを内部で発生すれば、上述した製造鍵は、必要でなくなることもある。しかし、もしコスト上の理由から望ましいのなら、鍵のペアは、PPE 650の製造時のみに曝されてもよいし、その時、製造鍵を用いて保護されてもよい。PPE 650がその公開鍵ペアを内部で発生できるようにすれば、この鍵ペアを隠すことが可能になる。しかし、ある種のアプリケーションでは、公開鍵の鍵ペア発生器をPPE 650内に導入することによるコストのほうが、より重要になることもある。

初期シークレット鍵

初期シークレット鍵は、初期化の間にPPEにダウンロードされた情報を保護するために、PPE 650に基づいて、シークレット鍵のみにより親鍵として用いられうる。この鍵は、PPE 650により発生され、PPEから、製造鍵を用いて暗号化された安全製造データベースへと送られる。この安全データベースは、これに応答し

て、初期シークレット鍵を用いて暗号化されたユニークなPPE製造IDを送り返す。

この初期シークレット鍵は、それがPPE初期化において果たす特殊な役割のために、「標準的な」暗号化に用いられる鍵よりもずっと長い鍵である可能性が高い。結果として復号化オーバーヘッドは、この初期化処理のあいだのみ生じるので、この鍵の選択された部分を用いて復号化ハードウェアを通る多数のパスは、許容可能である。

ＰＰＥ製造ＩＤ

PPE製造IDは、「鍵」ではなく、「共有秘密」の範疇定義内に入る。このIDは、好ましくは、PPE 650をユニークに識別し、PPE初期化処理の間にPPEの初期シークレット鍵を決定するために、安全データベース610により用いられうる。

サイトＩＤ、共有コード、共有鍵および共有秘密

VDEサイトIDは、共有コード、鍵および秘密と共に、好ましくは、PPE初期化処理の間にPPE 650へとダウンロードされるか、または、その処理の一部としてPPEにより内部で発生される。好ましい実施の形態では、この情報の大半または全部が、ダウンロードされる。

PPEのサイトIDは、PPE 650をユニークに識別する。このサイトIDは、好ましくは、PPE 650をユニークに識別し、かつそのPPEをその他すべてのPPEから区別することができるように、ユニークなものされる。このサイトIDは、好ましい実施の形態では、さまざまな目的（例えば、「アドレスプライバシー」機能の提供）に用いられうるユニークなアドレスを提供する。あるケースでは、このサイトIDは、PPE 650の公開鍵でありうる。別のケースでは、PPEのサイトIDは、製造および／または初期化処理の間に割り当てられうる。公開鍵の能力を持たないPPE 650の場合、デバイスのシークレット鍵をユニークなサイトIDとして用いることは望ましくないことがある。なぜなら、このことは、鍵のうちあまりにも多くのビットを曝すことになるからである。よって、異なる情報列をサイトIDとして用いるべきである。

共有コードは、制御プログラムのうちの少なくとも一部をPPE 650に提供する

、これらのコード断片を含んでいる。好ましい実施の形態では、PPE製造の間に、そのPPEがブートストラップし、初期化処理を始めることを可能にする基本コード断片がインストールされる。この断片は、初期化処理のあいだに、または後続するダウンロード処理のあいだに、更新された制御ロジックに置き換え可能である。

共有鍵は、初期化処理の間にPPE 650へとダウンロードされうる。これらの鍵は、例えば、多数のオブジェクト構造の秘密ヘッダを復号化するのに用いられうる。

PPE 650が、シークレット鍵のみのモードで動作している時、初期化およびダウンロード処理は、共有秘密をPPE 650へとインポートすることができる。これらの共有秘密は、通信処理の間に、PPE 650が、その他のPPEおよび／またはユーザのアイデンティティを認証できるようにするために用いられうる。

ダウンロード承認鍵

ダウンロード承認鍵は、初期化ダウンロード処理のあいだに、PPE 650により受け取られる。この鍵は、さらにPPE 650のコード更新、鍵更新を承認するのに用いられ、また、PPEの安全データベース610のバックアップを保護することによって、たとえPPEが故障しても（例えば）VDE管理者により復元可能とするためにも用いられうる。また、この鍵は、サイトID固有の鍵を導き出すために、サイトID、時間および旋回アルゴリズムと共に用いられうる。ダウンロード承認鍵は、また、安全データベース610のバックアップを暗号化するのに用いられた鍵ブロックを暗号化するのにも用いられうる。さらに、PPE 650への未来のダウンロードをイネーブルするのに用いられるサイト特異的な鍵をつくるのにも用いられうる。このダウンロード承認鍵は、好ましい実施の形態では、すべてのPPE 650の間で共有されるわけてはない。つまり、この鍵は、承認済みのVDE管理者によりおこなわれる機能に固有である。

外部通信鍵および関連する秘密および公開情報

PPE 650が通信するときに、鍵が必要になるいくつかのケースがある。安全

な通信を成立させる処理もまた、電子器具600との通信についての、関連する公開および秘密情報の使用を必要とすることもある。外部通信鍵およびその他の情報は、安全な通信をサポートし、認証するのに用いられる。これらの鍵は、好ましい実施の形態では、公開鍵のペアを含んでいる。ただし、共有シークレット鍵を、それの代わりに、またはそれに加えて用いてもよい。

管理オブジェクト鍵

好ましい実施の形態では、管理オブジェクト共有鍵は、管理オブジェクト870の秘密ヘッダを復号化するのに用いられうる。管理オブジェクトの場合、パーミッションレコード808が、秘密ヘッダに存在していてもよい。あるケースでは、パーミッションレコード808は、その他の管理オブジェクトの内容を処理する権利を提供する機能をおこなう管理オブジェクトとして（またはその中で）配付されうる。パーミッションレコード808は、好ましくは、秘密本文のための鍵を含んでいる。また、アクセスされうる内容のための鍵は、パーミッションレコード808で参照される予算でありうる。管理オブジェクト共有鍵は、時間を一成分として導入することができ、失効すれば、取り替えられうる。

静止オブジェクト鍵

静止オブジェクト共有鍵は、静止オブジェクト850の秘密ヘッダを復号化するのに用いられうる。既に説明したように、あるケースでは、パーミッションレコード808は、静止オブジェクトの秘密ヘッダに存在していることもある。もし存在しているのなら、このパーミッションレコード808は、秘密本文のための鍵を含んでいてもよいが、その内容のための鍵は含んでいない。これらの共有鍵は、時間を一成分として導入することができ、失効すれば、取り替えられうる。

移動オブジェクト共有鍵

移動オブジェクト共有鍵は、移動オブジェクト860の秘密ヘッダを復号化するのに用いられうる。好ましい実施の形態では、移動オブジェクトは、その秘密

ヘッダにパーミッションレコード808を含んでいることもある。このパーミッションレコード808は、好ましくは、秘密本文のための鍵と、パーミッションレコード808によりパーミッションが与えられる時にはアクセスされうる内容のため

の鍵とを含んでいる。これらの共有鍵は、時間を一成分として導入することができ、失効すれば、取り替えられうる。

安全データベース鍵

PPE 650は、好ましくは、これらの安全データベース鍵を発生し、それらをPPEの外部に決して曝すことがない。これらの鍵は、好ましい実施の形態では、サイト特異的であり、上述したように、「老化」されうる。上述したように、更新されたレコードが安全データベース610に書き込まれるたびに、新しい鍵を用いることができ、PPE内の鍵リストに載せておくことができる。周期的に(内部リストにもう余地がない時に)、PPE 650は、新しいまたは古いレコードを暗号化する新しい鍵を発生することができる。安全データベース610のサイズ次第では、単一の鍵の代わりに、鍵のグループを用いることもできる。

秘密本文鍵

秘密本文鍵は、オブジェクト300にユニークなものであり、PPE 650の間で共有される鍵情報には依存しない。これらの鍵は、好ましくは、秘密本文が暗号化される時にPPE 650により発生され、それらを「老化」させる一成分としてリアルタイムを取り入れることができる。これらの鍵は、パーミッションレコード808において受け取られ、その使用法は、予算により制御されうる。

内容鍵

内容鍵は、オブジェクト300にユニークなものであり、PPE 650の間で共有される鍵情報には依存しない。これらの鍵は、好ましくは、内容が暗号化される時にPPE 650により発生され、それらを「老化」させる一成分として時間を取り入れることができる。これらの鍵は、パーミッションレコード808において

受け取られ、その使用法は、予算により制御されうる。

承認共有秘密

PPE 650内または安全データベース610内の情報へのアクセスおよびその使用は、鍵ではなく、むしろ承認「共有秘密」を用いて制御されうる。承認共有秘密は、それらが承認するレコード(パーミッションレコード808、予算レコードなど)内に格納されうる。承認共有秘密は、対応するレコードが作成される時に書式

化（formulated）されうる。承認共有秘密は、承認PPE 650により発生されうる。また、レコードの更新が生じる時に取り替えられうる。承認共有鍵は、能力ベースのオペレーティングシステムにおいて用いられる「能力」に関連づけられた何らかの特性を有している。アクセスタグ（後述する）は、好ましい実施の形態では、重要な承認共有秘密セットである。

バックアップ鍵

上述したように、安全データベース610のバックアップは、安全データベースレコードのすべてと、PPE 650および外部の両方に格納されている現在の監査「ロールアップ」とを読み出すことからなる。その後、バックアップ処理は、発生された鍵の新しいセットを用いて、この情報を復号化し、再暗号化する。これらの鍵、バックアップ時刻、およびこのバックアップを識別するためのその他の適切な情報は、何度でも暗号化され、以前に暗号化された安全データベースファイルおよびロールアップデータと共に、バックアップファイル内に格納されうる。これらのファイルは、その後、PPE 650内で発生され、格納された「バックアップ」鍵を用いて、すべて暗号化されうる。このバックアップ鍵500は、もし必要であれば、PPEにより、バックアップを復元するのに用いられうる。これらのバックアップ鍵は、また、（例えば、ダウンロード認証鍵および／またはVDE管理者の公開鍵を用いて）安全に暗号化され、バックアップ自体の中に格納されることによって、PPE 650が故障した場合でも、VDEの管理者が、バックアップを復元できるようにする。

暗号化封印

封印は、情報が、偶然にまたはVDEの安全性への攻撃として、PPE 650の制御外で改変を受けうる時に、その情報の完全性を保護するために用いられる。具体的なアプリケーションを２つ挙げれば、データベースレコード用の検査値の計算と、SPE 500から交換されて出力された（swapped out）データブロックの保護とがある。

封印には２つのタイプがある。暗号化ハッシュ方式としても知られている鍵を用いない封印と、鍵を用いた封印の２つである。これらの両方とも、MD5やSHAの

ような暗号化的に強力なハッシュ関数を用いる。このような関数は、任意のサイズの入力を受け取り、固定されたサイズのハッシュすなわち「ダイジェスト」を生じる。このダイジェストは、同一のダイジェストを生じる２つの入力を計算することが実行不可能であり、具体的なダイジェスト値を生じる１つの入力を計算することが実行不可能であるという特性を有する。ここで、「実行不可能」であるとは、ビットで表されるダイジェスト値の大きさに基づく、仕事関数を参照していうものである。もし、例えば、256ビットのハッシュ関数を強力であると称するならば、複製された、あるいは指定されたダイジェスト値が生成される可能性が高くなるまでには、平均すると、およそ10^38（2^128）の試算を必要としなければならない。

鍵を用いない封印は、データベースレコード（例えば、PERC 808）および類似のアプリケーションにおいて検査値として用いられうる。鍵を用いない封印は、レコード本文の内容、およびレコードの残りの部分に格納されている封印に基づいて計算されうる。封印とレコードとの組み合わせは、記憶装置内でそれを保護するために、暗号化されうる。もし誰かが、暗号化鍵を知らずにその暗号化された鍵を（例えば、データを表す部分あるいは封印を表す部分を）改変すれば、復号化された内容は違ってくるし、復号化された検査値は、レコードのデータから計算されたダイジェストと一致しなくなる。たとえハッシュアルゴリズムが知られているとしても、レコードのデータおよびその封印を対応するように改変することは実行不可能である。なぜなら、それらの両方とも暗号化されているからである。

鍵を用いた封印は、暗号化なしに保護された環境の外部に格納されたデータに対する保護として用いられうる。また、２つの保護された環境間の有効性を示す証拠（validity proof）としても用いられうる。鍵を用いた封印は、鍵を用いない封印と同様に計算されるが、ただし、封印されているデータには、秘密初期値が論理的にプレフィクスされたものとして置かれる。よって、ダイジェスト値は、秘密およびデータの両方に依存しているので、データそのものは攻撃者に可視であるものの、改変されたデータに対応する新しい封印を計算することは、実行

不可能である。鍵を用いた封印は、単一の秘密値を用いて記憶装置内のデータを保護することができるし、あるいは、単一の秘密値を共有する２つの環境の間で遷移するデータを保護することもできる。

鍵を用いた封印あるいは鍵を用いない封印のいずれを選択するかは、保護されているデータの性格に依存しており、また、そのデータが暗号化によりさらに保護されるかにも依存している。

タグ付加

タグの付加は、重要なコンポーネントアセンブリの安全記憶装置および２次記憶メモリ652上の関連する情報をサポートするのに特に役に立つ。情報への「タグ付加」と暗号化戦略とを一体化して用いることにより、VDEノードの構成、管理および動作、ならびにVDEの保護された内容の使用を（部分的にはイネーブルするものの）限定し、および／または記録する情報を安全に格納する、安価な大容量記憶装置の使用が可能になる。

暗号化されているか、またはその他の手法により安全にされた情報が、ユーザの安全なVDE処理エリア（例えば、PPE 650）へと配送される時、この情報の一部は、「タグ」として用いられうる。このタグは、まず復号化されるか、さもなくば安全性が解除された（unsecured）後、予想された値と比較されることによって、その情報が予想された情報を表していることを確認する。よって、このタグは、受け取られ、VDE保護された情報のアイデンティティおよび正しさを確認する処理の一部として用いられうる。

好ましい実施の形態による制御構造に設けられうるタグには、以下の３つのクラスがある。

・アクセスタグ

・有効性検査タグ

・相関性タグ

これらのタグは、それぞれ別々の目的をもっている。

アクセスタグは、VDE保護されたエレメントと、（１つ以上の）タグの付加されたエレメントを読み出す、および／または改変することの承認されたエンティテ

ィとの間で「共有秘密」として用いられうる。このアクセスタグは、異なる複数のアクティビティをそれぞれ独立して制御するために、別々のフィールドに分解されてもよい。もしアクセスタグがメソッドコア1000のようなエレメントにより用いられるのなら、このようなエレメントに影響を及ぼす管理イベントは、影響を受けた（１つ以上の）エレメント用のアクセスタグ（またはそのアクセスタグの一部）を備えていなければならないし、イベントが処理にかけられる時には、そのタグをアサートしなければならない。もしアクセスタグが安全に保守され（例えば、エレメントが作成される時にPPE 650内部で作成され、暗号化された構造においてのみPPE 650から明らかにされ）承認済みのパーティのみに配付されるのなら、構造の改変は、さらに安全に制御されうる。もちろん、制御構造（例えば、PERC 808）は、管理イベントに現れる改変あるいはその他のアクションをさらに限定したり、その重要性を判定することができる。

相関性タグは、１つのエレメントが別のエレメントを参照する時に用いられる。例えば、作成者は、作成者のPERC内でその予算を参照する前に、パーミッションを得て、ビジネス関係を樹立することを予算所有者により要求されることがある。このような関係がつくられた後、予算所有者は、作成者に対して、予算所有者の予算を参照するPERCを生成することを許可する一つの局面として、１つ以上の相関性タグを作成者に送信することができる。

有効性検査タグは、改竄者側のレコード置換の企てを検出する一助とするために用いられうる。

いくつかの点で、これら３つのクラスのタグは、その機能面で重複している。例えば、相関性タグの不一致は、アクセスタグの検査がおこなわれる前に、アクセスタグの不一致により通常は防止されうる、あるクラスの改変の企てを防止することができる。好ましい実施の形態は、あるケースでは、例えば、アクセスタグを上述した有効性検査タグと同様の役割で用いることによって、オーバーヘッドを減らすために、この重複を利用することができる。

一般に、タグ付加プロシージャは、SPE 503内で、（１つ以上の）暗号化鍵と（１つ以上の）安全化技術とを変更することを伴い、および／または固有の、（１

つ以上の）格納されたタグを設けることを伴う。これらのプロシージャは、上述した安価な大容量記憶装置652内に格納されている情報であって、ハードウェアSPU 500内で、VDE保護された内容および管理データベース情報を用い、利用可能とすることによって、認証、復号化、またはその他の分析に利用される安全データベース610情報を用いておこなわれうる。通常、有効性検査タグの変更には、VDEノードのハードウェア（例えば、PPE 650）内に、タグの変更に対応する１つ以上の情報エレメントを格納することを伴う。ハードウェアSPEの物理的に安全で、信頼のおける環境の外部での情報の格納は、安全に格納をおこなう上でコストの大幅な削減を可能にする手段である。また、格納されている重要な管理データベース情報の安全性は、このように情報にタグを付加することによって、強化される。このようなタグの「変更」を頻繁に（例えば、ある与えられたレコードが復号化されるたびに）おこなえば、「正しい」情報が「正しくない」情報に置き換えられるのを防止することができる。なぜなら、このような置換は、後に情報を取り出す時に、ハードウェアSPEに格納されているタグ付加情報と一致する情報をもっていないからである。

情報にタグを付加することにより得られる別の効果としては、２つ以上のパーティの間で作用している情報および／または制御メカニズムを強要する、および／または検証する一助としてのタグの使用がある。もしあるパーティにより情報

にタグが付加された後、別の１つ以上のパーティに渡されたのなら、タグの付加されたその情報に関して、それら２つのパーティ間でおこなわれる通信および／または取引に関連づけられた、予想された値としてあるタグを用いることができる。例えば、もしパーティＡによりパーティＢに渡されるデータエレメントにあるタグが関連づけられるのなら、パーティＢは、そのデータエレメントに関連する情報（および／またはその一部）がパーティＢによりパーティＡへと明らかにされる前に、パーティＡに対して、そのタグの少なくとも一部について正しい値を知っていることを証明するように要求することができる（逆の場合も同様）。別の例では、タグは、パーティＢにより送られた情報が、タグの付加されたデータエレメント（および／またはその一部）に実際に関連づけられているかどうかを

検証するために、パーティＡにより用いられうる（逆の場合も同様である）。

安全で認証された通信チャネルの確立

２つのパーティ（例えばPPE ＡおよびＢ）は時折、両パーティにとって既知の通信チャネルを確立して、盗聴および不正改変がないこと、ならびにＩＤを互いに正確に知っているこれら２つのパーティによってのみ使用されていることを確実にする必要がある。

以下にこのようなチャネルを確立するプロセスの１つの例を述べ、セキュリティおよび認証のための要件がどのようにして確立され両パーティによって有効性が検査されるかを明らかにする。このプロセスは各パーティが確立しなければならないクレームおよび信用という用語で抽象的に述べられており、特定のプロトコルの仕様書としてみなされない。特に、各ステップの個々の下位ステップは個別の動作を用いて実現されるように要求されてはいない。実際には、関係するプルーフの確立および有効性検査は組み合わされて単一の動作とされることが多い。

下位ステップは、クレームが他方のパーティによってなされる前にはそのクレームの有効性を証明することはできないというような場合を除いては、以下に詳述する順序で行う必要はない。情報の「伝送」自体がいくつかの下位ステップに分割され得るため、ステップは、列挙された下位ステップにより暗示されるより多い、両パーティ間の追加の通信を含み得る。また、クレームまたはプルーフが伝送中に曝露または改変されないように保護する必要はない。クレームについての知識（特定の通信提案およびそれらの受け取り通知を含む）は保護情報であるとはみなされない。プルーフが改変されればそのプルーフは無効となりプロセスは失敗に終わる。

このプロセスを実現するために標準的な公開鍵または秘密鍵暗号技術（例えば、X.509、Authenticated Diffie-Hellman、Kerberos）を用いることができる。この好適な実施態様では、３方向X.509公開鍵プロトコルのステップが用いられる。

この例示したプロセスの最初の２つのステップは以下の通りである。

Ａ．（先駆ステップ）：Ａが有効性検査可能なクレームを作成する手段を確立する。

Ｂ．（先駆ステップ）：Ｂが有効性検査可能なクレームを作成する手段を確立する。

これら２つのステップにより、各パーティが、例えば、両パーティが秘密鍵を保持し、証明機関のデジタル署名によってそれ自体が認証される公開鍵を利用可能にする公開鍵署名スキームを用いることによって、他方のパーティにより有効性が検査され得るクレームを作成する手段が確実に得られる。

次のステップは以下の通りである。

Ａ（提案ステップ）：

１．ＢのＩＤを決定する。

２．Ｂにより作成されたクレームの有効性を検査する手段を得る。

３．この特定の提案された通信のための固有のＩＤを作成する。

４．両パーティおよび特定の通信を識別する通信提案を作成する。

５．ＡのＩＤおよび通信提案の出所の有効性検査可能なプルーフを作成する。

６．通信提案および関係するプルーフをＢに配送する。

これらのステップにより、対応するパーティＢのＩＤが確立され、通信が提案される。通信の確立にはＢによって作成されたクレームの有効性検査が必要となるため、Ａがこれらのクレームの有効性を検査する手段が提供されなければならない。通信の確立は、Ａによる通信のための特定の要件に固有のものでなければならないため、この通信提案およびすべての関係する交信は、他のこのような交信のすべてから明瞭に区別可能でなければならない。Ｂはその提案をＡからの正当な提案として有効性を検査する必要があるため、その提案が有効であるというプルーフを提供しなければならない。

次のステップは以下の通りである。

Ｂ（受け取り通知ステップ）

１．通信提案からＡのＩＤを抽出する。

２．Ａにより作成されたクレームの有効性を検査する手段を得る。

３．ＩＤおよび通信提案の出所についてのＡのクレームの有効性を検査する。

４．通信提案の固有のＩＤを決定する。

５．通信提案が前の提案の複写でないことを決定する。

６．この特定の通信提案を識別する受け取り通知を作成する。

７．ＢのＩＤおよび受け取り通知の出所の有効性検査可能なプルーフを作成する。

８．受け取り通知および関係するプルーフをＡに配送する。

これらのステップにより、パーティＢはＡの通信提案を受け取りこれについて行動する準備ができていることが確立される。Ｂは提案の有効性を検査する必要があるため、Ｂは先ずその出所を決定しその正当性の有効性を検査しなければならない。Ｂは、そのレスポンスが特定の提案に関係することおよびその提案がリプレイではないことを確実にしなければならない。Ｂは提案を受け入れる場合は、Ｂ自体のＩＤとＢが特定の提案を受け取ったことを証明しなければならない。次のステップは以下の通りである。

Ａ（確立ステップ）：

１．Ａの特定の提案に対するＢのクレーム受け取り通知の有効性を検査する。

２．受け取り通知から特定の通信提案のＩＤを抽出する。

３．受け取り通知が未解決の通信提案に関係することを決定する。

４．提案された通信に使用される固有のセッション鍵を作成する。

５．Ａがセッション鍵を作成したというプルーフを作成する。

６．セッション鍵が特定の通信提案と関係するというプルーフを作成する。

７．Ｂの受け取り通知を受け取ったというプルーフを作成する。

８．セッション鍵が伝送中に曝露されることから保護する。

９．セッション鍵が伝送中に改変されることから保護する。

１０．保護されたセッション鍵とすべてのプルーフをＢに配送する。

これらのステップにより、Ａはセッション鍵を特定して、これをＡの特定の通信提案に関連する今後のすべての交信に結びつけることができる。Ａは鍵を作成し、Ａがこれを作成したことを証明し、そしてこれが特定の提案された通信に連

結することを証明しなければならない。さらに、Ａはセッション鍵が提案を受け取ったというＢの受け取り通知に応答して生成されることを証明しなければならない。セッション鍵は曝露または改変から保護され、攻撃者が異なる値に換字することができないようにしなければならない。

VDE設備のPPE 650間の伝送可能性

１つの好適な実施態様では、VDEオブジェクト300および他の安全な情報は、適切であれば、上記に概略を示した様々な鍵を用いて、１つのPPE 650から別のPPE 650へ確実に伝送され得る。VDE 100はVDE管理情報の再配布を用いて、VDEオブジェクト300の所有権を交換し、オブジェクトの電子機器600間を移動を可能にする。

VDEオブジェクト300のパーミッション記録808は、オブジェクトの全体が、一部が、またはほんの少しが再配布され得るのかどうかを決定するために用いられ得る権利情報を含む。VDEオブジェクト300が再配布され得る場合は、電子機器600は、通常は、「予算」および／または機器がオブジェクトを再配布するのを可能にする他の許可するもの(permissioning)を持たなければならない。例えば、オブジェクトを再配布する権限が与えられた電子機器600は、機器が所有する予算または権利より少ないかまたはこれらに等しい予算または権利を含む管理オブジェクトを作成し得る。いくつかの管理オブジェクトは他のPPE 650に送られ得る。管理オブジェクトの１つを受け取るPPE 650は、関連するオブジェクトへの予算の少なくとも一部または権利を使用する能力を有し得る。

VDEオブジェクト300の所有権の移譲は、VDEオブジェクトのためのパーミッションおよび／または予算のすべてが異なるPPE 650に再配布される特別なケースである。VDEオブジェクトの中にはすべてのオブジェクト関連情報が配送されることを要求するものがあるかもしれない（例えば、すべての権利をオブジェクトに「売却」することは可能である）。しかし、VDEオブジェクト300の中にはこのような移譲を禁止しているものがあるかもしれない。所有権移譲の場合には、VDEオブジェクト300の最初の提供者は、所有権移譲が完了する前に、新しい所有者からの接触、移譲についての通知、および再承認を伴う承認共有秘密を用いた有

効性検査を必要とするかもしれない。

電子機器600が構成要素アセンブリを受け取るとき、アセンブリの暗号化部分は、アセンブリを供給したパーティまたはPPE 650しか知らない値を含み得る。この値は、最終的にはアセンブリ供給者に戻す必要がある情報（例えば、監査、課金および関連する情報）と共に保存され得る。構成要素供給者がその情報を報告するように要求すると、供給者はその値を提供し、これによりローカル電子機器600はこの値を最初に供給された値と比べてチェックし要求が正当であると確信することができるようにし得る。新しい構成要素が受け取られると、値は古い構成要素と比べてチェックされ、新しい構成要素が正当であるかどうかを決定し得る（例えば、次の報告プロセスで使用するための新しい値が新しい構成要素と共に含まれ得る）。

VDEセキュリティの完全性

PPE 650は多くのメソッドによって侵犯され得る。VDE 650によって提供されるセキュリティの目標は、システムが侵犯される可能性を減らし、侵犯された場合には悪影響を最小限にすることである。

VDE 100を実現するために用いられる基本的な暗号化アルゴリズムは安全である（暗号書記法においては強い）と仮定されている。これらには、コンテンツの秘密鍵暗号化、完全性検証のための公開鍵署名、PPE 650間またはPPEとVDE管理者間のプライバシのための公開鍵暗号化などが含まれる。これらのアルゴリズムへの直接の攻撃は、攻撃者の能力を超えると仮定されている。制御情報のための基本的な構築ブロックは十分に長い鍵を持ちまた十分に証明可能であるため、VDE 100の家庭用バージョンにとってはこれのいくつかは恐らくは安全な仮定である。

以下の脅しまたは攻撃のリスクは顕著であり得る。

・構成要素アセンブリ（例えば予算）の非承認の作成または改変

・コンテンツの非承認の大量曝露

・１つ以上の鍵の侵犯

・ハードウェアPPEのソフトウェアによるエミュレーション

・新しい記録に古い記録を換字

・「悪党」（すなわち本物ではない）ロードモジュールの導入

・リプレイアタック

・「指紋」の無効化

・個々のコンテンツ項目の非承認曝露

・個々のコンテンツ項目の再配布

１つ以上の暗号化鍵が侵犯されると、顕著な潜在セキュリティ侵害が起こり得る。しかし、上述のように、VDE 100によって用いられる暗号化鍵は十分に変動および区画化されているため、ほとんどの場合、１つの鍵を侵犯しても、攻撃者には制限された価値しか与えない。例えば、証明書秘密鍵が曝露されると、攻撃者は、上述のようにチャレンジ／レスポンスプロトコルを通過することはできるが、次のレベルのセキュリティに直面し、ここでは初期化チャレンジ／レスポンスまたは外部通信鍵のいずれかをクラックする必要がある。初期化チャレンジ／レスポンスセキュリティも無効にされると、初期化コードおよび様々な初期化鍵もまた曝露される。しかし、共有VDE鍵を見つけて鍵生成（「回旋」）アルゴリズムを複写するためにはコードおよびデータを理解する必要がある。さらに、正確なリアルタイムクロック値をだまし(spoof)によって維持しなければならない。攻撃者がこれすべてを成功裏に実現することができるならば、偽のPPEへの安全な通信すべてが侵犯され得る。オブジェクトのパーミッション記録808に関連する通信が偽のPPEに送られるならば、そのオブジェクトが侵犯され得る。

PPEダウンロード承認鍵と、安全データベース610のバックアップのための鍵を暗号化する鍵を引き出すために用いられるアルゴリズムとを知れば、特定の電子機器600の安全データベース全体が侵犯され得る。しかし、VDEオブジェクト300のコンテンツを侵犯するためにこの情報を用いるためには、適切なVDEの属性を理解することもまた必要となる。１つの好適な実施態様では、安全データベース610に格納された秘密の本体鍵およびコンテンツ鍵は、時間エレメントを含むことによって「老化」する。コンテンツを暗号化するのに必要な「本当の鍵」を得るために、時間が格納された値と共に回旋される。このプロセスもまた侵犯され

るならば、オブジェクトのコンテンツまたはメソッドが曝露され得る。この好適な実施態様では、承認されたVDE管理者の介入がなければ安全データベース610のバックアップはPPE 650に戻されないため、この情報を利用するためには「偽の」PPEを使用しなければならない。

この好適な実施態様では、外部通信共有鍵がサイトＩＤおよび時間に基づいた鍵回旋アルゴリズムと共に用いられる。侵犯される場合は、PPE 650との通信を可能にするのに必要なステップのすべてもまた知られ、この知識が利用されなければならない。さらに、復号化パーミッション記録808へのアクセスを得るためには管理オブジェクト共有鍵の少なくとも１つが侵犯されなければならない。

管理オブジェクト共有鍵を侵犯しても、「クラッカー」が外部通信鍵についての知識も持っているのでなければ価値はない。すべての管理オブジェクトは、共有外部通信鍵、サイトＩＤおよび時間を用いて交換される固有の鍵によって暗号化される。管理オブジェクトのコンテンツをさらに復号化するためには、PPE 650の内部詳細についての知識が必要となる。

静止オブジェクト（または同じ共有鍵を使用する他の静止オブジェクト）の秘密ヘッダは、侵犯された場合、共有鍵が「老化」して秘密ヘッダを復号化できなくなるまで攻撃者にコンテンツへのアクセスを提供する。オブジェクトの秘密本体もコンテンツも、そのオブジェクトのパーミッション情報808もまた侵犯されるまでは曝露されない。これらのオブジェクトの秘密ヘッダは、鍵が「老化」して秘密ヘッダを復号化できなくなるまで侵犯されたままである。

この好適な実施態様の安全データベース暗号化鍵は頻繁に変更され、またサイト特異的である。安全データベース610のファイルまたは記録の侵犯の結果は、侵犯された情報により異なる。例えば、パーミッション記録808は、VDEオブジェクト300の曝露本体およびコンテンツのための鍵を含む。パーミッション記録808が侵犯されると、「本当の鍵」を生成するアルゴリズムもまた知られている場合は、パーミッション記録によって提供される鍵によって保護されたこのオブジェクトの各面もまた侵犯される。秘密本体鍵が知られると、オブジェクトの秘密本体は、鍵が「老化」して期限切れとなるまでは侵犯される。この鍵の「老化」プ

ロセスも侵犯される場合は、侵害は永久に続く。秘密本体は、多くの異なるオブジェクトが共有するメソッドを含み得るため、これらのメソッドもまた侵犯され得る。侵害が検出されると、予算およびパーミッション記録を提供するすべての管理オブジェクトは侵犯されたメソッドを更新すべきである。安全データベース610に格納されているメソッドはより最近のバージョンに単に置き換えられ、従って更新が完了すると侵犯されたバージョンは使用不能になる。

コンテンツ鍵が侵犯される場合は、コンテンツのその鍵で暗号化された部分もまた、鍵が「老化」して期限切れとなるまで侵犯される。その鍵の「老化」プロセスも侵犯されると、侵害は永久に続く。多数レベルの暗号化が用いられているか、またはコンテンツの一部が異なる鍵で暗号化されている場合は、1つの鍵を知ってもコンテンツの一部またはすべてを解除するには十分ではない。

承認共有秘密（例えばアクセスタグ）が知られると、「クラッカー」がその秘密を適切に使用するメソッドを知っている場合は、その秘密を含む記録は承認された手段によって改変され得る。概して、外部通信鍵、管理オブジェクト鍵および管理ファイルもまた、共有秘密が有用となる前に「クラック」されていなければならない。当然ながら、この情報を利用するためにはプロトコルについての詳細な知識もまた必要となる。

この好適な実施態様では、PPE 650は侵犯されているかどうかを検出し得る。例えば、SPE 503に格納されている情報（例えば概要サービス情報）を安全データベース610に格納されおよび／またはVDE参加者（例えばVDE情報交換所）に伝送された情報と比較することによって、不一致が明らかとなる。PPE 650（またはその活動を見張っているかまたはこれと通信しているVDE管理者）が自らが侵犯されていることを検出すると、初期化により更新され、新しいコード、鍵および新しい暗号化／復号化アルゴリズムを用い得る。これにより、暗号化スキームが壊れたとき存在していたVDEオブジェクト300の曝露が制限される。新しいコードおよび鍵のダウンロードが行われない場合は、PPE 650に一定の期間後に機能を停止するように要求することが可能である。また、VDE管理者に更新を行うように強制することも可能である。また、新しいVDEオブジェクト300を得たいと望

むことで、ユーザに対して自分のPPE 650を規則的な時間間隔で更新しようという誘因が提供され得る。

最後に、一方の方向にはコンテンツ108が流れ、他方の方向には報告および請求書118が生成される、VDEアプリケーションの端と端とつなぐ(end-to-end)性質により、「裏－端」一致チェックを行うことが可能である。このようなチェックは情報交換所116で行われ、詐欺（例えば、対応する支払をせずに保護されたコンテンツを、そして対応する課金記録なしに使用記録を過剰に獲得すること）を示し得るかまたは実際に示す使用パターンを検出することができる。使用報告が詳細であること、ならびに使用記録および報告が電子形態で容易に利用可能であることにより、高度な詐欺検出メカニズムを構築し、これにより詐欺関連コストを受け入れ可能なレベルに維持することができる。

PPE初期化

各PPE 650は使用する前に初期化する必要がある。初期化は、製造業者のサイトで、PPE 650が現場に設置された後で、またはその両方で行われ得る。PPE 650の製造プロセスは、典型的には、装置を後でもっと完全に初期化し得る十分なソフトウェアをPPE内に埋め込むことを含む。この製造プロセスは、例えば、PPE 650内に永久に格納されるブートストラップローダーおよびチャレンジーレスポンスソフトウェアを試験すること、ならびにPPEの固有のIDをロードすることを含む。これらのステップにより基本的なVDE可能PPE 650が提供され、これは、（例えば、電子機器600内にインストールされ現場に設置された後）さらに初期化され得る。場合によっては、製造プロセスとさらなる初期化プロセスとを組み合わせて、「VDEインストレーション」PPE 650を製造してもよい。以上、図64および図65に関連して上述した概要をさらに詳細に述べた。

図68は、１つの好適な実施態様により行われ得るPPE 650を初期化するステップの例を示す。このフローチャートに示すステップのいくつかは、製造サイトで行われ得、いくつかはVDE管理者とPPE 650との間の接触を介して遠隔操作で行われ得る。もしくは、図に示すステップのすべてが製造サイトで行われるか、または図示したステップのすべてがPPE 500とVDE管理者との間の遠隔通信を介して行

われ得る。

初期化プロセス1370が製造サイトで行われる場合、PPE 650は先ず試験台に取り付けられる。製造試験台は先ずPPE 650を（例えばパワーオンクリアで）リセットし得る（ブロック1372）。このリセットが製造サイトで行われる場合は、PPE 650は、好ましくは、ソフトウェアの観点からPPEの動作を完全に試験し、PPEに異変があると失敗する特別な試験台ブートストラップコードを実行する。次に、好ましくは試験台ブートストラッププロセスの一部として提供される最初のチャレンジーレスポンス対話を使用して製造試験台とPPE 650との間に安全な通信交換が確立され得る。この安全な通信が確立されると、PPE 650は実行したブート

ストラップ試験の結果を製造試験台に報告し得る。PPE 650による試験が成功した場合は、製造試験台は新しいコードをPPE 650にダウンロードして内部ブートストラップコードを更新し（ブロック1376）、この結果、試験台は次にリセットを受けると試験台ブートストラッププロセスを最後まで行わない（ブロック1376）。製造試験台は次に新しいファームウェアをPPE内部の非揮発性メモリにロードし、これにより、追加の標準および／またはカスタマイズされた能力を提供する（ブロック1378）。例えば、製造試験台は、特定の製造ロットにとって適切なロードモジュールをPPE 650に予めロードしておいてもよい。このステップにより、PPE 500は特定のアプリケーションに対して工場でカスタマイズされ得る。

製造試験台は次に固有の装置IDをPPE 650にロードし得る（ブロック1380）。これによりPPE 650は固有のIDを所持し、これは次の対話で使用され得る。

この好適な実施態様では、ブロック1372～1380Rは典型的には製造サイトで行われる。ブロック1374および1382～1388は製造サイトで、PPE 650が設置された後で、または両方で行われ得る。

PPE 650をさらに初期化するためには、PPEと製造試験台またはVDE管理者との間に安全な通信が確立されると（ブロック1374）、必要な鍵、タグまたは証明書がPPE 650にロードされる（ブロック1382）。例えば、製造試験台はその情報をPPE 650にロードして、PPEが後で初期化され得るようにし得る。これらの値のい

くつかはPPE 650の内部で生成され得る。製造試験台またはVDE管理者はPPEリアルタイムクロック528を現在のリアルタイム値に初期化し得る（ブロック1384）。これにより、PPE 650のための時間および日付基準が与えられる。製造試験台またはVDE管理者は次にPPE 500の内部に維持されている概要値を初期化し得る（ブロック1386）。PPE 650が電子機器600の一部として既にインストールされている場合は、PPEはこの時点で安全データベース610を初期化し得る（ブロック1388）。

図69は、ファームウェアダウンロードプロセス（図68、ブロック1378参照）の一部としてPPE 650によって行われるプログラム制御ステップの例を示す。PPEダウンロードプロセスは、外部から提供されるファームウェアおよび／またはデータエレメントをPPEにロードするために用いられる。ファームウェアロードは2つの形態、すなわちPPE 650内にとどまるソフトウェアのための永久ロードと、

実行のためにロードされるソフトウェアのための短期ロードとを含む。安全データベース610に格納するための関連プロセスは、VDE電子機器600に送られたエレメントのために行われる。

PPE 650はいくつかのチェックを自動的に行って、PPEにダウンロードされているファームウェアがロードが完了する前に不正改変、置換または換字が行われていないことを確実にする。図に示すダウンロードルーチン1390はこのようなチェックの1つの例を示す。PPE 650が新しいファームウェア項目を受け取ると（ブロック1392）、この項目をチェックして、これが所定のダウンロードまたは管理オブジェクト鍵（エレメント源に依存する）を用いて適切に復号化されることを確かめる（決定ブロック1394）。ファームウェアが適切に復号化されると（決定ブロック1394の「YES」退出）、チェック値としてのファームウェアが計算され、ファームウェアの暗号化ラッパーの下に格納されているチェック値と比較され得る（決定ブロック1396）。これら2つのチェック合計値が同じ場合（決定ブロック1396の「YES」退出）、PPE 650はファームウェアに関係する曝露および秘密ヘッダ識別タグを比較して、適切なファームウェアが提供され換字されていないことを確かめる（このステップは図示せず）。この試験もまたパスする場合は、

PPE 500はファームウェアのディジタル署名（ディジタル署名がPPE 650によってサポートされ、ファームウェアが「署名」されていると仮定して）を計算し得、計算された署名をチェックして、ファームウェア暗号化ラッパーの下のディジタル署名と同じであることを確かめる（ブロック1398、1400）。これらの試験が1つでも失敗すると、ダウンロードは中断される（「失敗」終了1401）。

上記の試験のすべてにパスした場合、PPE 650は、ファームウェアをPPE内（例えば内部非揮発性メモリ）に格納するかどうか、または安全データベース610に格納するかどうかを決定する（決定ブロック1402）。ファームウェアをPPE内に格納する場合は（決定ブロック1402の「YES」退出）、PPE 500は単に情報を内部に格納し得る（ブロック1404）。ファームウェアを安全データベース610に格納する場合は（決定ブロック1402の「NO」退出）、ファームウェアには記録の換字を避けるために設計された固有のPPE特定タグが付けられ（ブロック1406）、次に適切な安全データベース鍵を用いて暗号化され安全データベース610に放出され得る（ブロック1408）。

SPU 500および／またはVDE電子機器600をネットワーク化

多くのコンピュータがローカルまたはワイドエリアネットワークによって相互接続される場合、それらのうちの1つまたは2～3のコンピュータがVDE電子機器600であることは有り得る。例えば、VDE可能サーバは1つ以上のSPU 500を含み得る。この集中化されたVDEサーバは、ネットワーク内で必要なすべてのVDEサービスを提供し得るか、またはVDEサービスをVDEサーバノードと共有し得る。すなわち、2～3の、いくつかの、またはほとんどのVDEサービス活動を行い得る。例えば、ユーザの非VDEコンピュータがVDE保護コンテンツを求める要求をネットワークを通じて発行するかも知れない。この要求に応答して、VDEサーバは、適切なVDEオブジェクト300にアクセスし、要求されたコンテンツを放出し、ネットワーク672を通じて要求したユーザにコンテンツを配送し得る。このようなアレンジメントにより、VDEの能力を、ネットワークに接続した様々なコンピュータおよび他の装置の改変または置換を必要とせずに現在のネットワークに容易に統合させることができる。

例えば、１つ以上の保護下の処理環境650を有するVDEサーバは、保護下の処理環境を持たないワークステーションとネットワークを通じて通信し得る。VDEサーバはすべての安全なVDE処理を行って、得られるコンテンツおよび他の情報をネットワーク内のワークステーションに放出し得る。このアレンジメントにより、ワークステーションはいかなるハードウェアまたはソフトウェアの改変も必要としない。

しかし、アプリケーションによっては、もっと高いセキュリティ、柔軟性および／または性能を必要とするものもあり、これは同じネットワーク672に多数のVDE電子機器600を接続することによって得られ得る。通常使用されるローカルエリアネットワークは、不正改変および／または盗聴が起こり得る安全でないチャネルを構成するため、最も安全なアプリケーションでは、ネットワークを横断して通信される情報を保護することが望まれる。VDE電子機器600と非VDE電子機器間をネットワーク672を横断して伝達されるVDE放出コンテンツまたは他のVDE情報を保護するために、従来のネットワークセキュリティ技術を用いることは可能であろう。しかし、同じシステム内に多数のネットワーク化されたVDE電子機器600を配備することによっていくつかの利点が得られる。

図８に関連して上述したように、多数のVDE電子機器600は、ネットワーク672または他の通信通路を通じて互いに通信し得る。このようなVDE電子機器600のネットワーク化にはいくつかの利点がある。例えば、VDE資源を集中化し、計量情報をサーバVDEに格納および／または集積し、そして情報およびサービスをネットワーク672を横断して多数の電子機器600に効率的に配送する可能性がある。

例えば、ローカルエリアネットワークのトポロジーでは、「VDEサーバ」電子機器600はVDE保護情報を格納し、これをネットワーク672を通じてサーバと通信し得る１つ以上の追加の電子機器600またはコンピュータに利用可能にし得る。１つの例としでは、VDEオブジェクトを格納しているオブジェクト格納場所が集中化サーバ内に維持され、多くのネットワーク化された電子機器600の各ユーザは、必要に応じてネットワーク672を通じて集中化されたオブジェクト格納場所にアクセスすることができる。ユーザが特定のVDEオブジェクト300にアクセスす

る必要があるときは、このユーザの電子機器600はネットワーク672を通じて要求を発行し、オブジェクトのコピーを得ることができる。「VDEサーバ」はこの要求に応答して要求されたオブジェクト300のすべてまたは一部を配送し得る。このような集中化されたオブジェクト格納場所728を提供することにより、ネットワーク672に接続した各電子機器600に対する多量格納要件を最小限にするという利点が得られ、同じ情報の冗長な複製がなくなり、情報管理の負担が緩和され、サーバで行われる特に重要なVDEプロセスおよび／または情報に対して物理的なおよび／または他のセキュリティがさらに提供される。このようなセキュリティをVDEノードで提供することは、ビジネスモデルによっては商業的に非実用的であり得る。

また、ローカルエリアネットワークのトポロジーで安全データベース610を集中化することは望ましい。例えば、ローカルエリアネットワークの場合、安全データベース610のサーバが中心位置に配備され得る。ローカルエリアネットワーク672に接続するいくつかの電子機器600のそれぞれは、ネットワークを通じて安全データベース610の記録を求める要求を発行し、ネットワークを介してこれらの記録を受け取り得る。記録はネットワークを通じて暗号化形態で提供され得る。記録を復号化するのに必要な「鍵」は、安全な通信交換でネットワークを横断して伝送することによって共有され得る。ネットワーク672内の安全データベース610を集中化することにより、ネットワーク化された電子機器600のそれぞれに対する二次格納および／または他のメモリ要件が最小限となるかまたは不要となり、冗長な情報格納が回避され、集中化したバックアップサービスが提供でき、情報管理の負担が緩和されるなどの潜在的な利点が得られる。

ネットワークを横断してVDE電子機器600を低コストて便利よく配置する多くの事例を得るための１つのメソッドは、ネットワークのワークステーションにHPE 655を定義するソフトウェアを配備することであろう。このアレンジメントはワークステーションのハードウェア的な改変を必要としない。HPE 655はソフトウェアのみを用いて定義され得る。SPE 503および／またはHPE 655もまたVDEサーバ内に配備され得る。このアレンジメントは、ワークステーションをカスタマイ

ズも改変もする必要なく、配布されたVDEネットワーク処理（新しいプログラムのロードを除く）が可能であるという利点を有する。高レベルのセキュリティを必要とするVDEの機能は、SPUベースのVDEサーバに制約され得る。「安全な」HPEベースのワークステーションはもっと低レベルのセキュリティを必要とするVDE機能を行い、またその活動をVDEサーバと調和させ得る。

従って、同じネットワーク内に多数のVDE電子機器600を配備することは有利であり得る。また、同じワークステーションまたは他の電子機器600内に多数のVDE電子機器600を配備することもまた有利であり得る。例えば、電子機器600は、多数の電子機器600を含み得、これらのそれぞれはSPU 500を有しVDEの機能を行うことができる。

例えば、１つ以上のVDE電子機器600はコンピュータシステムの入出力装置として使用され得る。これにより、１つの装置内で情報を復号化し、これを非暗号化形態でバスまたは他の安全でないチャネルを通って周辺装置などの別の装置に移動させる必要がなくなる。周辺装置自体がSPU 500を有するVDE電子機器600である場合は、VDE保護情報は、周辺装置での処理（例えば復号化）のために安全でないチャネルを通って周辺装置に確実に送られることができる。周辺装置にVDE保護情報を直接扱う能力を与えても柔軟性が増大する。例えば、VDE電子機器600の周辺装置は、VDEオブジェクト300の使用を制御し得る。例えば、装置が処理する情報に関係する使用または他のパラメータを計量し得、またVDEオブジェクトの使用についてもっと多くの情報を集めるために、装置が行う処理に特異的な監査トライアルおよび他の情報を集めてもよい。多数の協働するVDE電子機器600を配備することにより、暗号化された情報をVDE電子機器600に移し次に再びこれを非暗号化形態で非VDE装置に移す必要がなくなるため、性能が向上し得る。VDE保護情報は目的の装置に直接移され得、この目的の装置がVDE可能であれば、他のVDE電子機器600を巻き込む必要はなく情報を処理し得る。

図70は、多数のVDE電子機器600(1)、600(2)、600(3)、...、600(N)を有するアレンジメント2630の例を示す。VDE電子機器600(1)...600(N)は通信通路2631（例えば、ワークステーションのシステムバス、電話線または他のワイヤ、ケーブル

、バックプレイン、ネットワーク672、または他の通信メカニズム）を通じて互いに通信し得る。図示する電子機器600のそれぞれは、図８に示すのと同じ一般的な構造を有し得る。すなわち、それぞれCPU（またはマイクロコントローラ）654、SPU 500、RAM 656、ROM 658、およびシステムバス653を含み得る。図示する電子機器600のそれぞれは、インタフェース／コントローラ2632（これは図８に示す特定の種類のI／Oコントローラ660および／または通信コントローラ666であると考えられ得る）を有し得る。このインタフェース／コントローラ2632により、電子機器システムバス653と適切な電気コネクタ2634との間のインタフェースが提供される。電子機器600(1)、...600(N)のそれぞれの電気コネクタ2634は、共通のネットワーク672または他の通信通路への接続を提供する。

図示する電子機器600はほぼ類似の構造を有するが、異なる特殊なタスクを行い得る。例えば、電子機器600(1)は、ワークステーションの全体的な動作を管理し計算資源を提供する責任を負うワークステーションの中央処理部を備え得る。電子機器600(2)は、同じワークステーションのための多量記憶装置620であり得、例えば二次記憶装置652から情報を読み出しこれに情報を書き込み得る格納メカニズム2636を備え得る。電子機器600(3)は、表示タスクを行う責任を負う表示装

置614であり得、グラフィックスコントローラおよび関係するビデオまたは他の表示装置などの表示メカニズム2638を備え得る。電子機器600(N)は、関連するタスクの印刷を行うプリンタ622で有り得、例えば印刷メカニズム2640を含み得る。

電子機器600(1)、...600(N)のそれぞれは、すべてが共通のハウジング内に含まれる同じワークステーション装置の異なるモジュールを備えるか、または各電子機器は異なるシステム構成要素内に位置し得る。例えば、電子機器600(2)は、ディスクコントローラユニット内に配置され得、電子機器600(3)は表示装置614のハウジング内に配置され得、電子機器600(N)はプリンタ622のハウジング内に配備され得る。図７を参照して、スキャナー626、モデム618、遠隔通信手段624、キーボード612および／または音声認識ボックス613はそれぞれ、それ自体のSP

U 500を有するVDE電子機器600を備え得る。別のいくつかの例では、RFまたは無線インタフェースコントローラ、直列インタフェースコントローラ、LANコントローラ、MPEG（ビデオ）コントローラなどが含まれる。

電子機器600(1)...600(N)はそれぞれVDE可能であるため、それぞれVDE保護情報の暗号化および／または復号化を行う能力を有する。これは、ネットワーク672または電子機器に接続する他の通信通路2631を横断して伝達される情報はVDE保護され得ることを意味する（例えば、上述のように、情報はVDE管理および／またはコンテンツオブジェクトの形態でパッケージ化され暗号化される）。このアレンジメントの結果の１つは、通信通路2631を盗聴する盗聴者はVDE保護形態で得る以外には情報を得ることができないということである。例えば、電子機器600(1)によって生成される印刷される予定の情報は、VDEコンテンツオブジェクト300でパッケージ化され、通路2631を通じて印刷用電子機器600(N)に伝送される。この情報は保護形態で伝送されるため攻撃者はこの情報を横取りしても利益はほとんどない。非保護形態のときにこの情報にアクセスするためには、電子機器600(1)または600(N)（もしくはSPU 500(1)、500(N)）を侵犯しなければならない。

図示したアレンジメントで提供される別の利点は、電子機器600(1)、...600(N)のそれぞれは各自の計量、制御および／または他のVDE関連機能を行い得ることである。例えば、電子機器600(N)は、計量および／または印刷される情報に関連する他のVDE制御機能を行い得、電子機器600(3)は、計量および／または表示

される情報に関連する他のVDE制御機能を行い得、電子機器600(2)は、計量および／または多量記憶手段620に格納および／またはこれから取り出される情報に関連する他のVDE制御機能を行い得、そして、電子機器600(1)は、計量および／または処理する情報に関連する他のVDE制御機能を行い得る。

１つの特定のアレンジメントでは、電子機器600(1)、...600(N)のそれぞれは、電子機器によって受け取られるかまたはこれに送られる情報は、その機器のSPU 500を用いて次の情報を処理することであることを示すコマンドを受け取り得る。例えば、電子機器600(N)は、印刷のために受け取ろうとしている情報はVDE保護形態であることを示すコマンドを受け取り得る（または機器に送られる情報

自体がこれを示す）。このコマンドまたは情報を受け取ると、電子機器600(N)は、SPU 500を用いて受け取った情報を暗号化し、またSPUが印刷のために印刷メカニズム2644に提供する情報を計量し得る。復号化プロセスを不能にするために電子機器600(N)に追加のコマンドを送ってもよい。または、600(N)のVDE安全下位システムが、情報は復号化および／または印刷すべきではないことを決定し得る。追加のコマンドは、例えば、暗号化／復号化鍵をロードするために、「制限」をロードするために、「指紋」要件を確立するために、および計量された使用を読み出すために存在し得る。これらの追加のコマンドは必要に応じて暗号化または非暗号化の形態で送られ得る。

例えば電子機器600(1)が情報を作成しこれをVDE可能プリンタ622によって印刷したいと望むとする。SPU 500(1)は、通路2631を通じてSPU 500(N)と安全な通信を確立して、SPU 500(N)にデータの次のブロックを復合化しこれを復号化鍵および制限として格納するように命令するコマンドを提供し得る。SPU500(1)はさらにSPU 500(N)に復号化鍵および関係する制限を用いてこれに続く暗号化されたプリントストリームを処理するように命令するコマンドを送ってもよい（もしくは、このコマンドはCPU 654(1)によってマイクロコントローラ654(N)に送られ得る）。電子機器600(1)は次に、プリンタ622による復号化および印刷のために暗号化情報を通路672に送ることを開始し得る。プリンタ622が新しい情報ブロックを受け取るたびに直ちにSPU 500(N)は先ず制限がゼロより大きいことを確かめる。SPU 500(N)は次に維持している使用計量値を増分して制限値を減分する。制限値がゼ

ロでない場合は、SPU500(N)は受け取った情報を復号化して、これを印刷のために印刷メカニズム2640に提供する。制限がゼロの場合は、SPU500(N)は受け取った情報を印刷メカニズム2640に送ることもこれを復号化することもしない。停止せよというコマンドを受け取ると直ちにプリンタ622は「非安全」モードに戻り得る。このモードでは、プリンタは、VDE処理を許可せずに通路2631を通じて受け取ったものすべてを印刷する。

プリンタ622に関係するSPU 500(N)はプリンタのハウジング内に配置する必要

はなく、代わりに例えばI/Oコントローラ660内に配置し得る（図８参照）。これにより、上述の利点と同様の利点の少なくともいくつかが特別なVDE可能プリンタ622を必要とせずに提供され得る。もしくは、SPU 500(N)はプリンタ622内とプリンタと通信するI/Oコントローラ660内の両方に配備され得、I/O制御に調和し、中央処理電子機器600(1)と関係するSPU 500から処理負担をなくするという点で利点を提供し得る。１つの電子機器内に多数のVDE事例が生じるときは、１つ以上のVDE安全下位システムが「中央」下位システムであり得る。すなわち、「二次の」VDE事例は、暗号化された使用関連情報を１つ以上の安全な中央下位システムに通し、これによりこの中央下位システムが使用関連情報の格納を直接制御することができる。一定の制御情報はまた中央下位システムによって中央に格納され得、このような情報のすべてまたは一部は、その安全なVDE要求に応じて二次の安全下位システムに確実に提供される。

携帯電子機器

本発明によって提供される電子機器600は携帯型であり得る。図71は携帯電子機器2600の１つの例を示す。携帯機器2600は、１つの例ではほぼクレジットカードサイズであり得る携帯ハウジング2602を含み得る。ハウジング2602は、例えば１つ以上の電気コンタクトピン（図示せず）を有する電気コネクタ2604を介して外部世界に接続し得る。コネクタ2604は、ハウジング2602の内部の外部バスインタフェース2606をホストシステム2608の対のコネクタ2604aに電気的に接続させ得る。外部バスインタフェース2606は、例えば、PCMCIA（または他の標準）バスインタフェースを備え、携帯機器2600がバス2607を通じてホストシステム2608とインタフェースおよび通信することを可能にする。ホスト2608は、例えば、コンピュータ、有料電話、別のVDE電子機器600、テレビ、ゲームセンターのビデオゲーム、または洗濯機など想像し得るほとんどすべての機器であり得る。

ハウジング2602は不正改変を防止し得る（上記のSPUバリアー502の不正改変防止に関する記述を参照）。

この好適な実施態様の携帯機器2600は、ハウジング2602内に配置され得る１つ以上のSPU 500を含む。SPU500は、ハウジング2602内のバス2610によって外部バ

スインタフェース2606に接続され得る。SPU 500はこの内部バス2610を通じて（外部バスインタフェース2606を介して）ホスト2608と通信する。

SPU 500は、好ましくはハウジング2602内に配置されるバッテリ2612または他の携帯用電源によって電力供給される。バッテリ2612は、例えば、腕時計またはクレジットカードサイズの計算器に見られるタイプの小型バッテリであり得る。バッテリ2612は、太陽電池、再充電可能バッテリ、容量性蓄電池などによって補完（または交換）され得る。

ランダムアクセスメモリ(RAM)2614は好ましくはハウジング2602内に配備される。RAM 2614はSPU 500に接続され得るが、バス2610には直接は接続されない。このため、RAM 2614のコンテンツはSPUによってのみアクセスされ、ホスト2608によっては（SPUによって許可された場合にこれを通して行う場合を除いて）アクセスされない。図９に示すように、RAM 2614はSPU 500内のRAM 534の一部であり得る。但し、必ずしも同じ集積回路またはSPUの残りの部分を収容する他のパッケージ内に含まれる必要はない。

携帯機器2600のRAM 534は、例えば、携帯機器の各事例を個別に識別するために用いられ得る情報を含み得る。この情報は、認証、検証、復号化および／または暗号化プロセスで（例えば、鍵またはパスワード情報の少なくとも一部として）用いられ得る。

１つの実施態様では、携帯機器2600はVDE電子機器600の実質的にすべての機能を行う手段を備え得る。従って、例えば、携帯機器2600は、パーミッション、メソッド、鍵、プログラムおよび／または他の情報を格納し使用する手段を含み得、「スタンドアロン」型VDEノードとして作動し得る。

別の実施態様では、携帯機器2600は、追加の外部電子機器600に連結されると、好適な実施態様のVDE機能を行い得る。データベース管理パーミッション、メソッド、鍵および／または他の重要な情報（管理、ユーザインタフェース、分析などの他のVDEプログラムの少なくとも一部など）のような一定の情報は、（例えば記録として）携帯機器2600と情報を共有し得る外部VDE電子機器600に格納され得る。

不正改変を防止し得る携帯機器2600アレンジメントのための１つの可能な「スタンドアロン」構成としでは、１つ以上のプロセッサ（500、2616）および／または他の計算装置および／または他の制御ロジック、ならびにランダムアクセスメモリ2614を有する不正改変防止可能なパッケージ（ハウジング2602）を含む。プロセッサ500、2616は、完全に携帯機器2600内で（または少なくともその一部で）パーミッションおよびメソッドを実行し得る。携帯機器2600は、情報がハウジング2602の外部に伝達される前に情報を暗号化する、および／または情報がハウジングの外部から受け取られるとき受け取った情報を復号化する能力を有し得る。このバージョンの機器はまた、パーミッション、メソッドおよび／または鍵情報の少なくとも一部を非揮発性メモリの上記不正改変を防止し得る携帯ハウジング2602内に確実に格納する能力を有し得る。

携帯機器2600の別のバージョンは、携帯機器2600の外部のローカルVDE電子機器600からパーミッションおよび／またはメソッドおよび／または鍵を得て、VDE保護オブジェクトのユーザによる使用を制御、制限さもなくば管理し得る。このような携帯機器600は、別の電子機器2600内に含まれるか、これによって受け取られるか、この内部にインストールされるか、もしくはこれに直接接続され得る。

携帯域2600の「極小」構成の１つの例は、SPU 500およびバッテリ2612をハウジング2602内に含み得る（この場合には、外部バスインタフェース2606およびRAM 2614はそれぞれ図示するSPUブロックに組み込まれ得る）。携帯機器2600の他のもっと高度な例では、以下のオプションの構成要素のいずれかまたはすべてもまたハウジング2602内に含まれ得る。

１つ以上のCPU 2616（RAM-ROM 2617、I/Oコントローラ（図示せず）などの関係するサポート構成要素と共に）、

１つ以上の表示装置2618、

１つ以上のキーパッドまたは他のユーザ入力ボタン／制御情報2620、

１つ以上の取り外し／交換可能なメモリ装置2622、および

１つ以上の印刷装置2624。

このような高度なバージョンでは、表示装置2618、キーパッド2620、メモリ装置2622およびプリンタ2624はバス2610に接続され得る。もしくは、CPUのI/Oポート／コントローラ部（図示せず）を介してCPU2616に接続され得る。表示装置2618はSPU 500、CPU 2616および／またはホスト2608からの情報を表示するために用いられ得る。キーパッド2620は、SPU 500、CPU 2616および／またはホスト2608に情報を入力するために用いられ得る。プリンタ2624は、これらの供給源のいずれか／すべてからの情報を印刷するために用いられ得る。取り外し／交換可能なメモリ2622は、メモリカートリッジまたはバルク記憶装置などのメモリ媒体を備え、追加の長期または短期の格納を提供する。メモリ2622は、所望であればハウジング2602から容易に取り外され得る。

１つの実施態様では、携帯機器2600は、「スマートカード」のフォームファクターを有し得る（「スマートカード」フォームファクターはいくつかの利点を提供し得るが、ハウジング2602のフォームファクターは「従来の」スマートカードと同じであってもこれとは異なってもよい）。もしくは、このような携帯電子機器2600は、例えば、パーソナルコンピュータにおいて現在極めて有名になりつつあり、デスクトップ型計算装置およびPersonal Digital Assistantsにおいて一般的になると予想されるPCMCIAカード構成（など）でパッケージ化され得る。携帯電子機器ハウジング2602のための１つの有利なフォームファクターは、例えば、クレジットカードまたはこれより幾分大きい寸法のタイプ１、２または３のPCMCIAカード（もしくはこれから派生した他のもの）であり得る。このようなフォームファクターは好都合に携帯可能であり、広範囲のコンピュータおよび消費者用機器に、さらに、小売店および銀行などの商業施設で、ならびに電話または他の遠隔通信「ブース」などの公衆通信地点のレセプタクルに挿入可能であり得る。

ハウジング2602は、ポート、スロットまたは他のホスト2608によって提供されるレセプタクルに挿入またこれから取り外しされ得、これによりコンピュータまたは他の電子機器に物理的に（さもなくば作動可能に）接続され得る。携帯機器コネクタ2604は容易に取り外し可能なように構成され得、これにより機器2600は

異なる位置の別のコンピュータまたは他の電子機器まで移動させて、その装置と物理的な接続または他の作動可能な接続を行い得る。

携帯電子機器2600は、ユーザが、ノートブック型コンピュータ、デスクトップ型コンピュータおよびオフィスコンピュータ間などの（互換の）様々な電子機器600間でパーミッションおよびメソッドを移動させる貴重な比較的簡単な手段を提供し得る。また、例えば、消費者が隣人の家を訪問し、その消費者が鑑賞のライセンスを取得している映画を隣人に見せるか、または恐らく消費者が無制限再生のライセンスを取得している大容量光ディスクでの音声記録を隣人に聴かせるためにも使用され得る。

携帯電子機器2600はまた、ユーザが例えば商業用アプリケーションなどの他の様々なアプリケーションで用いる金融および他の取引のための「スマートカード」としても機能し得る。携帯電子機器2600は、例えば、商業プロセスおよびサービスを承認（および恐らく記録）するために用いられるパーミッションおよび／またはメソッドの情報を所持し得る。

この好適な実施態様のVDE携帯機器2600を典型的には銀行およびクレジットカード会社によって行われるような金融取引のために使用することの１つの利点は、VDEは金融情報交換所（VISA、MasterCardまたはAmerical Expressなど）が運転コストを著しく削減することができることである。情報交換所でコストを低減し得るのは、携帯機器2600などのVDE電子機器600を使用することによりユーザサイトでローカルな計量および予算管理が行われるため、取引毎に情報交換所が巻き込まれることがなくなるからである。現在の要件とは対照的に、情報交換所は記録を定期的に（月一回など）更新することによってその機能を行うことができる。監査および／または予算の「巻き上げ」は、このような監査および／または予算情報を伝達するために起動された接続の間に、および／または定期的なまたは比較的定期的な間隔で行われる接続を介して、および／またはクレジット更新、購入、もしくは他の携帯機器2600の取引の間に行われ得る。

情報交換所VDEディジタル配分取引は、はるかにコストのかかる各セッション中の接続ではなく、時折の承認および／または中央サービスへの監査または他の

管理の「巻き上げ」を必要とするだけである。クレジットカード購入の「書面による追跡」（クレジットカード伝票の承認および転送）を維持する必要はないため、通信コスト、情報の同時処理を扱う設備、および取引処理コストの書面扱い部分の低減により、情報交換所での実質的なコスト低減（および潜在的にはユーザのコスト低減）が実現され得る。このように携帯機器2600を使用することにより、各VDE電子機器600の計算能力を用いる配分処理を開発するクレジット実施が可能になる。これらのクレジットコストおよび処理面での利点はまた、非スマートカードおよび非携帯型VDE電子機器600の使用にも適用され得る。

VDE 100は高度に安全な商業環境として構成され得るため、そしてVDEによってサポートされる認証プロセスは、紙面書類および手書きの署名と同等の公式の有効性検査を提供するディジタル署名プロセスを用いるため、費用のかかる取引においても、携帯機器2600が紙面による追跡を維持する必要はなくなる。監査可能な課金および制御メカニズムがVDE 100内に組み込まれ自動化されているため、VISA、MasterCard、AMEXおよび銀行の借方アカウントへの従来の電子インタフェースを、ディジタル配分された他の製品およびサービスに置き換え、情報交換所での実質的な運転コストを節約し得る。

所望であれば、携帯機器2600は、消費者に対して携帯電子履歴を維持し得る。携帯履歴は、例えば、コンピュータまたは他の消費者ホスト機器2608の電子「ドック」または他のレセプタクルに移動されるか、またはこれに作動可能に接続され得る。ホスト機器2608は、例えば、マイクロコンピュータの形態で少なくとも一部に制御ロジックを有し、例えば税金および／または他の取引カテゴリー（使用または活動タイプなど）により組織化されたメソッドで情報を格納するする電子オーガナイザであり得る。このアレンジメントを用いることによって、消費者はレシートさもなくば手動による追跡取引を維持する必要はなく、それにもかかわらず、取引および取引明細書の非常に安全な電子監査追跡を維持することができる。取引明細書は、例えば、ユーザのディジタル署名および、選択により、サービスまたは商品提供者のディジタル署名を確実に含み得る。

携帯機器2600が、パーソナルコンピュータまたは他の電子機器（電子オーガナ

イザなど）のようなホスト2608に「ドック」されるときは、携帯機器2600はホストに中間監査情報を伝達することができる。１つの実施態様では、この情報は、直接にまたは間接に、コンピュータまたは電子オーガナイザおよび／または税金管理プログラム（例えば、QuickenまたはMicrosoft Moneyおよび／またはTurbo Taxおよび／またはAndrew Tobias' Managing Your Money）に読み出すことができる。このレシート管理の自動化は消費者にとっては大層な恩恵であり得る。なぜなら、レシートの管理および保守は困難で時間が掛かり、レシートは無くなったり忘れられたりすることが多く、そしてクレジットカード課金は通常は購入項目についての十分なデータまたは有意な取引パラメータを提供しないため、クレジットカード課金の詳細は課金および返済のためには概して不十分であることが多いからである。

１つの実施態様では、携帯機器2600は、VDE電子機器600を含むかもしくは小売業者または第三者の提供者のVDE電子機器600と通信し得る小売端末と安全な（この例では暗号化および／または認証された）２方向通信をサポートし得る。例えば各参加者の安全なVDE下位システム間のこのような安全な２方向通信の間に、各携帯機器2600の安全なVDE下位システムは、認証および適切なクレジットまたはデビットカード情報を小売端末のVDE安全下位システムに提供し得る。同じまたは異なる通信セッションの間に、端末は同様に携帯機器2600のVDE安全下位システムに、小売取引に関する詳細（例えば、購入商品および価格、小売施設のディジタル署名、小売端末の識別子、税金関係情報など）を確実に送り返し得る。

例えば、携帯機器2600を受容するためのおよび／またはこれに接着するためのホスト2608のレセプタクルは、小売店または他の商業施設の端末に組み込まれるかまたはこれに作動可能に接続され得る。ホスト端末2608は、商業施設の従業員または携帯機器2600の保持者のいずれかによって操作され得る。例えば、ホスト端末は誰がディナーに招待されたか、何故購入したか、または各情報が属するカテゴリーなどの特定の情報を特定のキーボードおよび／または音声入力するために用いられ得る。情報は次に自動的に「解剖」され、携帯機器2600内の確実に維持された（例えば暗号化された）適切なデータベース管理記録へと通路が定められる。これら「解剖」およびルーティングはVDE安全下位システムプロセスによ

って確実に制御され、例えば、ユーザによって入力されたカテゴリー情報および／または施設のクラスおよび／または出費情報（または他の使用）のタイプ（カテゴリー）に基づくものとされ得る。カテゴリー化は、例えば、電子カテゴリー情報を例えば電子レシート情報の一部として確実に伝達することによって、もしくはプリンタ2624を用いてハードコピーレシートを印刷することによって、小売店によって提供され得る。このカテゴリー化のプロセスは、携帯機器2600で行われ得るか、もしくは小売店によって行われ定期的に携帯機器2600の保持者に「巻き上げ」られ通信される。

小売店、情報交換所または他の商業組織は、情報に記録への解剖を自動化するために、および／またはデータベース情報「巻き上げ」のために、および／または携帯機器2600または1つ以上の関係するVDEノードにおいて用いられ得る（例えば政府の徴税規則によって特定されているような）取引タイプの1つ以上の一般的な分類を、機器2600に確実に伝達することによって維持および使用し得る。このような例では、ホスト2608は例えば補助端末を備えるか、もしくは、商業施設キャッシュレジスターまたは他の小売取引装置を備えるか、またはこれに直接組み込まれ得る。補助端末はメニューおよび／またはアイコンにより駆動され得、ユーザは非常に容易にカテゴリー化の選択を行うことができる。また、取引タイプによっては、有用なまたは必要な取引に特異的な情報（例えば、ビジネスディナーの目的および／またはディナーの出席者）を特定することによりユーザを誘導することができるテンプレートを提供し得る。例えば、ユーザはビジネスアイコンを選択して、例えば出張、販売、食事、管理または購入アイコンを選択し、非常に特異的な情報および／またはキーワードもしくは他のコードを入力して、取引の詳細を携帯機器2600にダウンロードすることができる。この情報はまた、商業施設によって格納され得、そして報告された取引の有効性検査のために適切な政府および／またはビジネス組織に伝達され得る（高レベルセキュリティのVDEの監査、通信、認証および有効性検査は十分に信頼され、平行監査履歴の維持を必要としないようにすべきであるが、平行維持はサポートされ、少なくとも限られた期間は維持されるため、携帯機器2600および／または履歴および／または状態情報記録維持のために機器2600によって使用される1つ以上のVDE装置260

0

に関係するVDEインストレーションが失われるかまたは「故障」した場合にはバックアップ情報を提供し得る。例えば、小売端末が維持する機器2600を巻き込む取引に関する必要な取引情報については、小売端末はこのような情報を保管（および／または他の行為）のために情報交換所に伝達するか、または、定期的に、例えばビジネス日の終わりに、このような情報を例えばVDEコンテンツコンテナオブジェクトの形態で情報交換所または情報交換所エージェントに確実に伝達し得る。このような取引履歴（および利用可能なクレジットなどのすべての必要なVDE関連状態情報）は維持され得、必要であれば、携帯機器2600内で情報を再構築して、機器2600のユーザに置換機器を配備するか、またはデータ内の内部情報を適切にリセットするために用いられ得る。このとき、このような置換および／またはリセットはすべての必要な取引および状態情報を提供する。

小売店では、補助端末ホスト2608は、例えば食事の終わりにユーザに提示される携帯装置の形態を取り得る。ユーザは自分の携帯機器2600をPCMCIAスロットなどのスマートカードレセプタクルに挿入して追加の情報を入力する。この情報は、取引を適切に説明し、また必要とされる電子機器600識別手順を満たすものであり得る。十分なクレジットが利用可能な場合は、取引は認められ、取引関連情報は補助端末から直接携帯機器2600に戻される。これはクレジット使用および記録管理の非常に便利なモードである。

携帯装置補助端末は「オンライン」であり得、セルラー、衛星、無線周波数または他の通信手段を用いることにより商業施設および／または第三者の情報収集ポイントに電子的に返送される。補助端末は、収集ポイントでの一定の識別情報の受け取りに応答して商業パーティによってチェックされた後、クレジット記録が不良であることまたは携帯機器2600の盗難などの他の情報に基づいて携帯機器2600を受け入れるかどうかを補助端末に返送し得る。このような携帯補助端末はまた、他の商業施設、例えばガソリンステーション、レンタルカー返却領域、街やスタジアムの売り子、バー、ならびに店員および他のスタッフが従来のキャッシュレジスタの位置以外の地点での取引を完了させ得ることによって効率が最適

化され得る他の商業施設でも非常に有用であり得る。

上述のように、携帯機器2600は、時折、例えばVDE管理者などの他の電子機器600と通信し得る。携帯機器2600使用セッション中の通信は、接続が携帯機器の使用の現在のセッション（もしくは次のまたは他のセッション）中に行われるように指示する内部に格納されたパラメータに基づく。携帯機器600は、適切であれば、（例えば、恐らく取引またはそのセッションのためにユーザによって考慮された他のプロセス前に、その間に、またはその直後に）通信を行うことを要求するリアルタイムの日付または時間帯もしくは期間に関する情報を所持し得る。このような通信は直ちに実現され得、安全なVDE２方向通信であり得、この通信の間、情報は中央情報取り扱い者に伝達される。一定の他の情報は携帯機器2600および／または携帯機器2600が接続しているコンピュータまたは他の電子機器に伝達され得る。このような伝達された他の情報は、考慮されたプロセスが進行するのを可能にするかまたは阻止し、および／または携帯機器2600を少なくとも一部は使用不能にまたは使用可能にし得る。携帯機器2600に伝達される情報は、１つ以上の予算のリセットまたは増加、一定ののパーミッションの追加または削除などのパーミッションおよびメソッドへの１つ以上の改変を含み得る。

携帯機器2600によって所持されるパーミッションおよび／またはメソッド（すなわち予算）は、別の、静止の、または他の携帯VDE電子機器600の「負担」に関連して割り当てられたものであり得る。１つの実施態様では、携帯機器2600の保持者または他のVDE電子機器600および／またはVDE電子機器600のユーザは、別のパーティによって行われる取引の金融面の「保証人」として働き得る。保持者の携帯機器2600は「負担」を記録し、これは、情報交換所との安全な通信中は、他方のパーティの債務責任のすべてまたは一部が支払われるかもしくは満たされるまで、情報交換所および／または他の金融サービスパーティによって記録および維持され得る。もしくはまたはこれに加えて、負担はまた携帯機器2600内に維持され得、保証人の付随債務を表す。形式によっては、負担は保証人に利用可能なクレジットの決定に含まれ得る。クレジットの移譲、受け入れおよび／または記録管理ならびに関連プロセスは、本発明の局面によって提供されるセキュリティ

特性によって確実に維持され得る。携帯機器600は、１つ以上のVDEオブジェクト300のためのパーミッションおよび／またはメソッドにとっての唯一の場所であり得る。もしくは、携帯機器は、別の非携帯型VDE電子機器600で見出されるこれらオブジェクトのための予算から独立したこれらオブジェクトのための予算を所持し得る。これにより、予算は、例えば、「負担」および予算の調停を必要とせずに移動可能となる。

携帯VDE電子機器2600は、（上述の他のVDE電子機器600と同様に）クレジット履歴詳細についての情報、承認の概要、および無コストまたは低コストで一定のVDE保護情報の再使用を可能にする使用履歴情報（例えば、取引履歴または一定のタイプ／クラスの情報の使用などの関連概要情報のある程度の監査）を所持し得る。このような使用または使用コストは、少なくとも一部は、VDE保護情報の１つ以上のオブジェクトまたはオブジェクトクラスの以前の使用、もしくは使用量などに依存し得る。

携帯機器2600はまた、少なくとも一部は、識別のために使用され得る一定の情報を所持し得る。この情報は、一定の順序（例えば、擬似乱数アルゴリズムに基づくパターン）で使用され、携帯機器2600の所持者のIDを検証し得る。このような情報は、例えば、自分自身のまたは妻のおよび／または他の親類の旧姓、自分自身のおよび／または他人の社会保障番号、誕生日、生まれた病院、および他の身元証明情報を含み得る。また、もしくは、音声プリントおよび網膜スキャン情報などの個人のIDを識別するかもしくは検証／認証するために用いられる１つ以上のパスワードまたは他の情報を提供または含み得る。例えば、携帯機器2600は、承認および予算のための様々なパーミッションおよび／またはメソッド情報を所持するスマートカードとして使用され得る。この情報は、安全データベース610アレンジメントの携帯機器2600内に確実に格納され得る。ユーザが電子機器を購入するかまたはライセンスを得ようとするとき、もしくは「スマートカード」を使用してプロセスを承認しようとするとき、携帯機器2600はユーザに自己証明情報を質問するか、もしくはスキャンまたは入力された情報（ユーザの指紋、網膜または音声分析、もしくは、例えば、提供された特徴の携帯機器2600内に確実

に格納されている情報へのマッピングおよび／またはマッチングを用い得る他の技術など）を用いる自己証明プロセスを開始し得る。携帯機器2600は異なる時間に異なる質問を用い得（および／またはスキャンするためのもしくは自己証明情報を入力するための複数の質問または要求を提供し得）、これにより、１つ以上の

ID「試験」のための適切な情報を所有した個人が携帯機器2600を成功裏に使用するのを妨げる。

携帯機器600はまた、例えば安全なVDE下位システム間の関連コンテンツの安全なVDE通信を用いて、電子通貨またはクレジットを他の携帯機器2600にまたは別の個人口座に振り替える能力を有し得る。このような振替は、例えば、クレジットおよび／または通貨を他の口座に振り替え得る銀行への遠隔通信または銀行に出向くことによって実現され得る。振替はまた、同じ携帯機器2600のドッキングステーションで２つのカードを用いることによっても行われ得る。例えば、クレジット取引ワークステーションは、２つのPCMCIAスロットおよび適切なクレジットおよび／または通貨振替アプリケーションソフトウェアを含み得る。このソフトウェアは、１つの携帯機器2600を確実に借方にし、別の携帯機器を「貸方」にすることができる（すなわち、一方の機器を借方にすることは、対応するクレジットおよび／または通貨を他方の機器に発行することにより生じ得る）。一方の携帯機器600は、例えば、別のユーザに認証されたクレジットを提供し得る。２つの「スマートカード」携帯機器600を用いることにより、「クレジット」「スマートカード」を提供するユーザは取引プロセスを無事通り抜けることができる。このプロセスでは、ユーザは適切な自己証明（例えばパスワード）を提供し、別の「スマートカード」携帯機器2600を識別する「公開鍵」を識別する。他方の携帯機器2600は受け入れプロセスを用い、ディジタル署名のための適切な自己証明を提供し得る（および、クレジットおよび／または通貨の送り元はまた、取引証明書にディジタル署名し得、これにより送付行為は否認されず、この証明書はVDEコンテナコンテンツとしてクレジットおよび／または通貨に添付し得る）。取引は、例えば、振替の利率および／または他の条件を規定するユーザインタフェ

ース対話を含み得る。クレジットの提供者がパーティ間の同意を記述する一定のパラメータについて質問される通常の取引タイプのためのテンプレートを用い得る。受信する携帯機器2600は、条件の受け入れについて繰り返してまたは全体として質問され得る。電子クレジットおよび／または通貨の別のVDEスマートカードまたは他のVDEインストレーションへのスマートカード振替において、本出願のどこかに記載したVDEネゴシエーション技術が用いられ得る。

このようなVDE電子機器600／携帯機器2600クレジット振替という特徴により、クレジットカードにより始められデビットカードにより拡張されたクレジット制御およびクレジット利用可能性の計算を拡張することを通じてこれらのプロセスを顕著に自動化することにより、一定の電子クレジットおよび／または通貨活動を管理する間接費が著しく低減され得る。クレジット拡張および／または通貨振替の自動化、ならびに上述の関係する配分処理の利点、さらに各取引中の集中化処理および遠隔通信のための要件がないことにより、多くの消費者および他の電子通貨および／またはクレジットユーザにとって、クレジットおよび／または通貨は実際に効率的で信頼性があり携帯可能な商品となる。

１つの実施態様では、携帯機器2600または他のVDE電子機器600はまた、多くの徴税機能を自動化し得る。VDE電子機器600は、高いセキュリティで、金融取引を記録し、取引の性質を識別し、必要なセールスまたは関連する政府の取引税を識別し、ユーザの利用可能なクレジットから税金を借方にし、そして一定の間隔で（例えば毎月）直接１つ以上の政府の代理機関にこの情報を確実に伝達し、および／または例えば金融情報交換所にこの情報を確実に転送し、情報交換所は１つ以上の安全な暗号化された（または安全でない、情報交換所によって計算された、もしくはコンピュータで計算された）情報監査パケット（例えば、VDEコンテンツコンテナおよび使用する安全なVDE通信技術）を、１つ以上の適切な参加政府代理機関に転送し得る。VDE 100の全体的な完全性およびセキュリティにより、税金関連情報の電子報告（１つ以上の電子商業活動から引き出される）は有効でわかりやすいことが、一貫した集中化されたメソッドによって確実となる。また、売上税徴収の振替についての情報の有効性を検査する源としても作用し得る

（例えば、資金が商業上の操作により政府に直接転送され、および／または報告された税金関連情報が税金情報を扱うVDE通路内の他のパーティによって不正改変され得ないようなメソッドで転送される。政府の代理機関は取引をランダムに選択するか、または一定の商業上の操作のために報告された取引のある部分またはすべてが選択され得る。これは、商業上の操作により税金に必要なすべての適切な徴収資金が実際に政府に支払われていることを確実にするために用いられ得、また、取引（銀行口座からの利子の受け取り、投資、贈与などを含む）に対する適

切な税金が最終ユーザに課されていることも確実となり得る。

携帯機器2600の金融および税金プロセスは、本明細書のどこかに記載したテンプレートメカニズムを含み得る。このような電子クレジットおよび／または通貨管理能力は、少なくとも部分的に携帯機器2600を使用することにより管理されるならば、特に興味深いものとなり得る一方で、クレジットおよび／または通過振替および類似の特徴はまた、非携帯型VDE電子機器600をコンピュータまたは他の電子装置に接続するかまたはこれの内部にインストールする場合にも適用可能である。

ユーザ通知除外インタフェース（「ポップアップ」）686

上述のように、ユーザ改変除外インタフェース(User Modification Exception Interface)686は、共通のVDE機能を扱うユーザインタフェースプログラムセットであり得る。これらのアプリケーションはVDEテンプレートの形態であり、特に、一定のVDEユーザモデルにとって適切な重要な選択、および報告された一定のイベントであるにちがいない重要なメッセージに関する一定の仮定に基づいて設計される。「ポップアップ」ユーザインタフェース686の主要な機能は、簡単な一貫したユーザインタフェースを提供して、例えば、計量イベントおよび除外（例えば、自動処理が不可能であるかまたは論証可能に望ましくない条件）をユーザに報告し、ユーザが自分の電子機器600の操作の一定のいくつかの面を構成するのを可能にし、そして、適切であれば、ユーザが一定の取引プロセスを進めるかどうかを対話式に制御するのを可能にすることである。オブジェクトが除外

扱いメソッドを含む場合は、このメソッドが、「ポップアップ」ユーザインタフェース686が特定のクラスの除外を如何に扱うかを制御する。

「ポップーユーザ」インタフェース686は、通常は、例えば以下に述べるような、特定のオブジェクト300に振り分けられないタスクを扱うことができる。

・電子機器600にログすること、および／またはVDEに関連する活動または活動クラスに入ること。

・登録ユーザのために、および／または一般に設置のために、ユーザの好みを考慮して電子機器600を構成すること、および一定のタイプの除外を自動的に扱うこと。

・適切であれば、ユーザが特定の特性と共に使用するための計器を選択すること。

・配給者からコンテンツを要求および／または購入もしくはリースすることを含む、他の電子機器600との通信のためのインタフェースを提供すること、情報交換所のクレジットおよび／または予算を情報交換所から要求すること、他の電子機器へ情報を送るおよび／または他の電子機器から情報を受け取ることなど。

図72Aは、ユーザインタフェース686を使用し得る共通の「ログオン」VDE電子機器600の機能の一例を示す。「ログオン」は、ユーザ名、口座名および／またはパスワードを入力することによって行われ得る。この例に示すように、「ポップアップ」ユーザインタフェース686ダイアログによって提供される構成オプションは「セットアップでのログイン」であり、これは、選択されれば、ユーザの電子機器600に電源が入るかまたはリセットされる度に自動的にVDEログイン手順を開始する。同様に、「ポップアップ」ユーザインタフェース686は、「タイプでのログイン」と呼ばれるインタフェースオプションを提供し得る。これは、選択されれば、例えば、一定のディレクトリのファイル、一定の自己証明拡張子を有するコンピュータアプリケーションまたはファイルなどの一定のタイプのオブジェクトまたは特定のコンテンツタイプのアプリケーションが開けられる度に自動的に手順を開始する。

図72Bは、ユーザによる行為が「トラップ」された場合に起動される「ポップ

アップ」ユーザインタフェース686ダイアログの一例を示す。この場合では、ユーザの行為によって掛かる出費額についてユーザに知らせ、また要求されたオブジェクト300についておよびこの特定のオブジェクトを使用するのに掛かる費用についてユーザに注意を促している。この例では、インタフェースダイアログは、全文記載、関係ファイルのリスト、および恐らくはオブジェクトまたは関係するディスカウントを使用する残された権利を含むオブジェクトの過去の使用の履歴を含む、オブジェクトについてのさらに詳細な情報をユーザが要求するのを可能にするボタンが提供され得る。

図72Bの「CANCEL」ボタン2660はユーザのトラップされた要求を取り消す。「CANCEL」はこの例ではこのダイアログのデフォルトであり、例えば、ユーザのキーボード612ではリターンおよびエンターキーによって、ボタンでは「マウスクリック」によって、音声コマンドによって、または他のコマンドメカニズムによって起動され得る。「APPROVE」ボタン2662は、マウスクリックまたは他のコマンド手順によって明確に選択されなければならないボタンであって、ユーザが費用を認め先へ進むのを可能にする。「MORE OPTIONS」制御2664は、ダイアログを、さらなるオプションを提供する別のレベルの詳細へと拡張する。この例を図72Cに示す。

図72Cは、図72Bの「MORE OPTIONS」ボタン2664がユーザによって選択されるとき、「ポップアップ」ユーザインタフェース686によってユーザに提示される二次ダイアログを示す。図示するように、このダイアログは、さらなる情報を得、様々なタスクを行うための多くのボタンを含む。

この特定の例では、ユーザは、例えば、セッションドル制限額（フィールド2666）、合計取引ドル制限額（フィールド2668）、時間制限（分）（フィールド2670）および「単位制限」（段落、頁などの単位数）（フィールド2672）などの「制限」を設定することが許される。ユーザが選択を完了すると、OKボタン（2674）を「クリック」して制限の選択を確認しこれらを有効にする。

従って、ポップアップユーザインタフェースダイアログは、１つのセッション中のまたは一定の期間にわたるもしくは一定の時間までの予算および／またはオ

ブジェクトコンテンツの使用の他の面について制限を設定するなど、ユーザの好みを特定するために提供され得る。ダイアログはまた、１つ以上のオブジェクトと共に使用される計器および予算を選択するなどのオブジェクト関係使用オプションを選択するためにも提供され得る。オプションの選択は、命令を、所望する１つ以上のタイプに関連する１つ以上の自己証明パラメータに関係付けることによって複数のタイプ（すなわちクラス）のオブジェクトに適用され得る。ユーザ特定構成情報は、様々な状況で使用されるべきデフォルト値を設定し得、またユーザによるオブジェクトの使用が「ポップアップ」インタフェース686ダイアログによって割り込まれる事態の頻度またはタイプを制限するために用いられ得る。例えば、ユーザは、要求された情報の処理が＄25.00を超えない場合、現在のセッション（および／または日、および／または週など）の全体に対する料金の合

計が＄200.00を超えない場合、ならびにユーザに対する未決および未払い料金の合計が＄2500.00を超えない場合、VDE保護コンテンツを求めるユーザの要求は（除外行為により生じる）割り込みなしに自動的に処理されるべきであると特定し得る。

ポップアップユーザインタフェースダイアログはまた、顕著な条件およびイベントについてユーザに知らせるために使用され得る。例えば、インタフェース686は以下のために用いられ得る。

・監査情報を情報交換所に送るようユーザに確認する。

・予算額が低く補充が必要であることをユーザに知らせる。

・安全データベース610をバックアップするようにユーザに確認する。そして

・PERCまたは他の日付／時間イベントの期限切れについてユーザに知らせる。

他の重要な「ポップアップ」ユーザインタフェース686の機能としては、ローカルに格納されているVDE保護オブジェクトからおよび／または１つ以上の様々な遠隔地のコンテンツ提供者からのライセンス取得または購入が可能なプロパティまたはオブジェクトのライブラリーを柔軟にブラウジングし得るダイアログを含む。このような機能は、ユーザのコンピュータが遠隔の配布者のまたは情報交

換所の電子機器600に接続されているときに、または選択（プロパティ、資源の位置、またはあるクラスのオブジェクトまたは資源などが選択される）の後に遠隔の供給源への電子接続を作動させることによって提供され得る。ブラウジングインタフェースにより、ユーザが項目を選択するとこの電子接続が自動的に行われるか、または接続自体がユーザによって明確に作動され得る。このような「ブラウジング」ダイアログの一例として図72Dを参照せよ。

スマートオブジェクト

VDE 100はその制御能力および特徴を「情報エージェント」に拡張する。一般に、「情報エージェント」は密使として働き、この密使を派遣するプロセスが最初のプロセスが特定する結果を実現するのを可能にする。派遣プロセスが存在しないときに行動し得る情報エージェントは、派遣プロセスが遠隔の電子機器の資源にそのエージェントを介してアクセスするのを可能にするために特に有利である。このようなシナリオでは、派遣プロセスは、特定の所望のタスクを特定するエージェント（例えば、コンピュータプログラムおよび／またはコンピュータプログラムに関係する制御情報）を作成し、このエージェントを遠隔システムに派遣し得る。遠隔システムに到達すると、「エージェント」は、遠隔システムの資源を用いて指定されたタスクを実行し得る。これにより、派遣プロセスは、このプロセスが存在しない遠隔システムにその能力を実質的に拡張することができる。

このようにして「エージェント」を用いることにより柔軟性が増大する。派遣プロセスは、遠隔システムには存在しないかまたは利用できない特定の所望のタスクをエージェントを介して特定することができる。また、このようなエージェントを用いることにより信用度がさらに増大する。派遣プロセスは遠隔システム全体ではなくそのエージェントだけを「信頼」すればよい。

ソフトウェアエージェントは、高レベルの制御および説明義務（accountability）が有効、安全且つ有用であることを必要とする。コンピュータウィルスの形態のエージェントは世界中に破壊的な影響をもたらしている。従って、エージェントがアクセスすることを許すシステムは、エージェントを制御し得るか、さもな

くばエージェントが重要な資源に損害を与えるのを防ぐべきである。さらに、エージェントがアクセスするのを許すシステムは、エージェントを十分に信頼し、および／またはエージェントの活動に責任があるエージェントの本当の派遣者を保持し得るメカニズムを備えるべきである。同様に、派遣プロセスは、派遣するエージェントの権威を十分に制限および／または制御し得るべきである。さもなくば、エージェントによる不測の活動に対して責任を負うべきである（例えば、エージェントは、エージェントを派遣したプロセスによって引き続いて与えられる不正確な命令により莫大な額の請求書をためることになるかもしれない）。

ソフトウェアエージェントを用いる場合のこれらの顕著な問題は過去に十分に取り組まれていない。VDE 100によって提供される開放的で柔軟性のある制御構造は、ソフトウェアエージェント（例えばエージェントオブジェクト）のための所望の制御および説明義務を提供することによってこれらの問題に取り組む。例えば、VDE 100はコンテンツアクセスおよび使用を積極的に制御し、使用されるコンテンツのための支払いの保証を提供し、アクセスされたコンテンツのための

予算制限を実施する。これらの制御能力は、派遣されたエージェントの活動をエージェントを派遣するプロセスおよび派遣されたエージェントによってアクセスされる資源の両方によって制御するのによく適している。

本発明によって提供されるこの好適な実施態様の１つの局面は、エージェントを含む「スマートオブジェクト」を提供する。一般に、「スマートオブジェクト」は、VDE電子機器600でVDE制御情報と共に使用するためのあるタイプのソフトウェアプログラム（「エージェント」）を含むVDEオブジェクト300であり得る。基本的な「スマートオブジェクト」は、例えば以下のものを（物理的におよび／または仮想として）含むVDEオブジェクト300を備え得る。

ソフトウェアエージェント、および

ソフトウェアエージェントの動作を支配する、エージェントに関係する少なくとも１つの規則および／または制御。

「スマートオブジェクト」を定義するにはこの基本構造で十分であるが、図73は、ソフトウェアエージェントの動作を確実に管理および制御するための特に有利

なスマートオブジェクト構造の一例を提供する、コンテナと制御情報との組み合わせを示す。

図73に示すように、スマートオブジェクト3000はコンテナ300により構成され、コンテナ内には、１つ以上のさらに別のコンテナ（300z、300yなど）が埋め込まれている。コンテナ300はさらに、これらの埋め込まれたコンテナ300z、300yなどにアクセスしこれらを用いるための規則および制御情報を含み得る。コンテナ300に埋め込まれたコンテナ300zは、オブジェクト3000を「スマートオブジェクト」にするものである。これはVDE 100によって管理および制御される「エージェント」を含む。

コンテナ300zに関係する規則および制御情報806fは、例えば実行コストに基づく実行の制限を含む、エージェントが遠隔のVDEサイトで放出され実行され得る環境を支配する。この規則および制御情報は全くコンテナ300z内で特定され得、および／またはコンテナ300の一部として、または別のコンテナの一部として（コンテナ300内または別個に送達可能なコンテナ）として送達され得、および／または遠隔VDEサイトに既に存在し得る。

第２のコンテナ300yはオプションであり、コンテナ300zに格納されたエージェントが実行され得る位置を記述するコンテンツを含む。コンテナ300yはまた、コンテナ300yのコンテンツが使用されるかまたは改変されるメソッドを記述する規則および制御情報806eを含み得る。この規則および制御情報806eおよび／またはコンテナ300y内に含まれるさらに別の規則300y(1)は、スマートオブジェクト3000を所望の遠隔情報資源に向けるために使用され得る検索およびルーティングメカニズムを記述し得る。コンテナ300yは、検索およびルーティングの使用および変更に対して支払いを行い得るメソッドを特定する規則および制御情報300y(1)を含み得るおよび／または参照し得る。

コンテナ300xはオプションのコンテンツコンテナであり、スマートオブジェクト3000が遠隔サイトに派遣されるとき最初は「空」である。これは、コンテナ300zに含まれるエージェントの実行によって取り出されるコンテンツを格納するための規則および制御情報300x(1)を含む。コンテナ300xはまた、検索コンテナに

格納されているコンテンツの値についての制限も含み、これにより検索されるコンテンツの量を制限する。

コンテナ300内の他のコンテナは、コンテナ300zのエージェントの行動および遠隔VDEノードでエージェントを実行させるために掛かる料金を記述する監査および課金追跡を含む管理オブジェクトを含み得る。スマートオブジェクト3000の正確な構造は、制御されるエージェントのタイプ、実行のために必要とする資源、および検索される情報のタイプに依存する。

図73に示す例のスマートオブジェクト3000は、VDE 100内のエージェントの動作を制御および管理するために用いられ得る。図74に示すスマートオブジェクト取引の例についての以下の詳細な説明は、理解を助けるものではあるがこれに限定されない。この特別な例では、ユーザは、「非常に速くて効率的な(Very Fast and Efficient)」ソフトウェアエージェントを用いてライブラリ検索を行い、興味ある主題（例えば「fire flies（蛍）」）について書かれた本を検索するスマートオブジェクト3000を作成しようとしていると仮定する。検索手段は本のリストをユーザに戻すように設計されている。この例での検索手段は、適切な本を見つけるのに$10.00を超えない金額を使い、ライブラリに入るためのライブラリアクセスまたは通信料金に$3.00を超えない金額を使い、そして情報の検索に$15.00を超えない金額を使う。検索または使用に関連するすべての情報はユーザに戻され、ユーザは、ユーザまたはエージェントに属する情報が第三者に放出されるのを認めない。

この例では、派遣するVDE電子機器3010は、図73に示すスマートオブジェクトに類似するスマートオブジェクト3000を構成する。806aの規則セットは、以下のエレメントを含む制御セットとして特定される。

１．スマートエージェントが埋め込まれたコンテナ300zに格納されこのコンテナで特定される実行を制御する規則を有するということを特定するsmart_agent_executionイベント、

２．スマートエージェントがコンテナ300に格納されている情報およびパラメータを用いて作動することを特定するsmart_agent_useイベント、

3．情報ルーティング情報がコンテナ300yに格納され、このコンテナに格納されているこの情報を制御する規則を有することを特定するrouting_useイベント、および

4．書かれた情報がそのタイプ（ルーティング、検索または管理）に依存してコンテナ300y、300xまたは300wに格納され、これらのコンテナは情報をどのように書くかを制御する個別の規則を有することを特定するinformation_writeイベント。

制御セット806bの規則セットは、このスマートオブジェクト3000によって所望される権利を特定する規則を含む。特に、この制御セットは、ソフトウェアエージェントが以下のものを所望することを明示する。

1．遠隔VDEサイトで「エージェント実行」サービスを使用する権利。この権利のための特定の課金および料金情報はコンテナ300zに所持される。

2．遠隔VDEサイトで「ソフトウェア記載リスト」サービスを使用する権利。このための特定の課金および料金情報はコンテナ300yに所持される。

3．遠隔VDEサイトで「情報ロケータサービス」を使用する権利。

4．情報を無料（情報の放出に掛かる料金、支払いはVISA予算によって行われる）でユーザに戻す権利。

5．監査情報すべてを送り元によってのみ可読な形態で戻す権利。

制御セット806cの規則セットは、コンテナ300wがその使用に関連するすべてのイベントの扱いを特定することを明示する。制御セット806dの規則セットは、コンテナ300xがその使用に関連するすべてのイベントの扱いを特定することを明示する。制御セット806eの規則セットは、コンテナ300yがその使用に関連するすべてのイベントの扱いを特定することを明示する。制御セット806fの規則セットは、コンテナ300zがその使用に関連するすべてのイベントの扱いを特定することを明示する。

コンテナ300zは、「非常に速くて効率的な」エージェントコンテンツを含むものとして特定され、これは以下の規則セットに関連する。

1．実行を所有者のVISAカードに対して請求される$10.00に制限する計量器

およびVISA予算を特定する使用イベント。使用の監査が必要とされ、これはオブジェクト300wに、このオブジェクトで特定される制御情報の下で格納される。

コンテナ300zおよびそのセットが特定された後、これらはスマートオブジェクトコンテナ300内で構成されこれに埋め込まれる。

コンテナ300yは、２つのタイプのコンテンツを有するコンテンツオブジェクトとして特定される。コンテンツタイプＡはルーティング情報であり、本質的に読出し／書込みが行われる。コンテンツタイプＡは以下を特定する規則セットに関係する。

１．コンテンツの放出のためのいかなる動作も特定しない使用イベント。これはコンテンツの使用に対して料金の請求がないという効果を有する。

２．書込みの値を＄３.００に制限する計量器およびVISA予算を特定する書込みイベント。書込みによって用いられる課金メソッドは特定しないでおき、この規則を使用する制御メソッドによって特定され得る。

３．使用の監査が必要とされ、オブジェクト300wに、このオブジェクトに特定される制御情報の下で格納され得る。

コンテンツタイプＢはソフトウェアエージェントによって使用され、エージェントのためのパラメータを特定する。このコンテンツは文字列「fire fly」または「fire flies」として特定される。コンテンツタイプＢは以下の規則セットに関係する。

１．使用はソフトウェアエージェントまたはルーティングエージェントによってのみ行われることを特定する使用イベント。ソフトウェアエージェントは読出しのみのパーミッションを有し、ルーティングエージェントは情報への読出し／書込みアクセスを有する。情報の使用に関係する料金の請求はないが、２つの計量器、読出しによるものと書込みによるものがプロセスの様々なステップによって情報の使用を追跡するために保持される。

２．使用の監査が必要とされ、オブジェクト300wに、このオブジェクトに特定される制御情報の下で格納され得る。

コンテナ300yおよびその制御セットが特定された後、これらはスマートオブジ

エクトコンテナ300内で構成されこれに埋め込まれる。

コンテナ300xは、コンテンツが空であるコンテンツオブジェクトとして特定される。これは以下の規則を含む制御セットを含む。

１．書込みの金額を＄15.00に制限する計量器および一般予算を特定するwrite_without_billingイベント。

２．使用の監査が必要とされ、オブジェクト300wに、このオブジェクトで特定される制御情報の下で格納され得る。

３．所定のメソッド（メソッドオプション）を用いて情報の所有者によって満たされ得る空の使用制御セット。

コンテナ300xおよびその制御セットが特定された後、これらはスマートオブジェクトコンテナ300内で構成されこれに埋め込まれる。

コンテナ300wは、以下の規則を含む制御セットにより空の管理オブジェクトとして特定される。

１．管理オブジェクトに含まれる情報はスマートオブジェクトコンテナ300の作成者にのみ放出され得ることを特定する使用イベント。

２．コンテナ300wの管理コンテンツにはいかなる他の規則も付けられない。

コンテナ300wおよびその制御セットが特定された後、これらはスマートオブジェクトコンテナ300内で構成されこれに埋め込まれる。

この時点で、スマートオブジェクトの構成は完了し、遠隔VDEサイトに派遣される準備が整っている。スマートオブジェクトは（例えば、電子メールまたは他の伝送メカニズムを用いて）通路3014を介して情報ロケータサービス3012を含む遠隔VDEサイトに送られる。スマートオブジェクトは「項目ロケータサービス」のための遠隔サイト3012で登録される。「項目ロケータサービス」に関連するコンテナの制御セットが選択され、この中に含まれる規則が遠隔サイト3012で起動される。遠隔サイト3012は次に、コンテナ300yのコンテンツを規則セット806「および300y(1)の制御の下で読み出し、これらの規則に従ってローカル情報リストをコンテナ300yに書き込むのを許可する。項目ロケータサービスは三つの項目よりなるリストをスマートオブジェクトに書き出し、次にスマートオブジェクト（

この時点では位置情報を含んでいる）を「再登録」し、これを、通路3018を介してスマートオブジェクトに書き込まれたリストで特定されたサイト3016に送る。この例では、ユーザは伝送のための特定の電子メールを有し得、所望の情報を有し得る遠隔サイトのリストが転送リストとして格納される。

第２の遠隔サイト3016に到着すると、スマートオブジェクト3000はこの第２のサイトに登録される。サイト3016は、スマートオブジェクトへのサービスとしてVDEと互換性のあるエージェント実行およびソフトウェア記述リストサービスを提供する。このサイトはこれらのサービスを公表し、エージェントを開始するのに＄10.00、そしてすべての情報を戻すのに単位当たり＄20が必要であることを特定する。登録プロセスは、公表されたサービス情報をオブジェクト内に格納されている規則と比較し、受け入れ不可能な重複は存在しないと決定する。これらの活動すべての監査情報が管理オブジェクト300wに書き込まれる。登録プロセスは失敗し（オブジェクトは登録されず）、スマートオブジェクトはサイト3016によってリストの次のVDEサイト3020に通路3022を介して転送される。

第３の遠隔サイト3020に到着すると、スマートオブジェクト3000はこのサイトに登録される。サイト3020は、スマートオブジェクトへのサービスとしてVDEと互換性のあるエージェント実行およびソフトウェア記述リストサービスを提供する。このサイトはこれらのサービスを公表し、エージェントを開始するのに＄1.00、そしてすべての情報を戻すのに単位当たり＄0.50が必要であることを特定する。登録プロセスは、公表されたサービス情報をオブジェクト内に格納されている規則と比較し、受け入れ可能な重複が存在すると決定する。登録プロセスは、同意された制御情報を特定するURTを作成する。このURTは他の制御情報と合わせて用いられ、VDE制御下でソフトウェアエージェントを実行する。

エージェントソフトウェアは始動しコンテナ300yからそのパラメータを読み出す。次に、データベースの検索を開始し、データベースの253個の「ヒット」を得る。ヒットリストが、各項目の細分性および各項目の料金が＄0.50であることを特定する完全制御セットと共に、コンテナ300xに書き込まれる。検索が完了すると、サービス使用のための予算は＄1.00だけ増加し、このサービスの使用料金

を反映する。これら活動のすべてに対する監査情報は管理オブジェクト300wに書き込まれる。

遠隔サイト3020は、「満杯」になったスマートオブジェクト3000をVDEノード3010で通路3024を介して最初の送り元（ユーザ）に戻す。スマートオブジェクト3000は登録されデータベース記録が利用可能となる。コンテナ300xで特定された制御情報は、この時点では、最初の制御情報とこれらの情報の遠隔放出に関するサービスによって特定された制御情報との混合である。ユーザは次にスマートオブジェクト3000から20個の記録を抽出し、抽出時に$10.00がVISA予算に請求される。

上記のスマートエージェントVDEの例では、スマートオブジェクト3000およびこれを構成するコンテナの一定の組織について述べた。他のVDEおよびスマートオブジェクト関連制御情報およびパラメータデータの組織も作成され得、上記の例のオブジェクト3000に帰する目的と同じ目的のために使用され得る。

ネゴシエーションおよび電子契約

電子契約は、契約を結ぶパーティの権利、制約および義務を含む契約の電子形態である。多くの場合、電子契約とはディジタルで提供されるコンテンツの使用を取り巻くものであり得、例えばディジタルで配布される映画を鑑賞するための許可書が挙げられる。しかし、電子契約は、契約を結ぶ一つ以上のパーティによって電子コンテンツの存在または使用について条件付けられる必要はない。この最も簡単な形態では、電子契約は権利およびこの権利がどのように行使されるか

を支配する制御を含む。

電子契約は、従来の契約のように、パーティ間でネゴシエートされ得る（１つ以上のパーティによって提出される条件は、一つ以上の他のパーティによって単に受け入れられる（コヒーレント契約）、および／またはこの他のパーティはこのような条件のいくつかを選択する（その他の条件は必須）権利を有し得る）。ネゴシエーションは、辞書では「相互の同意によって和解する行為」と定義されている。この好適な実施態様では、一つ以上の権利および関係する制御が自動化された条件の電子ネゴシエーションを介して確立され得る電子ネゴシエーション

プロセスが提供される。ネゴシエーションは、通常は、権利の正確な特定とこれらの権利に関係する制御とを必要とする。PERCおよびURT構造は、権利の正確な電子表現およびこれらの権利に関係する制御を提供するために使用され得るメカニズムを提供する。従って、VDEは、ユーザおよび作成者が両者の所望を特定し得る「ボキャブラリ」およびメカニズムを提供する。自動化されたプロセスはこれらの所望を解釈し、これらの所望に基づく共通の中間地点に到達するようにネゴシエートする。このネゴシエーションの結果は構造体に簡潔に記載され、これが電子契約の結果を制御および実施させるために使用され得る。VDEは、ネゴシエーションプロセスがその動作における完全性および秘匿性を確実にする安全な実行スペースを提供することによって、このプロセスをさらに可能にする。ネゴシエーションプロセスはまた、ネゴシエーションが外部から不正改変されるのを防ぐようなメソッドで実行され得る。

一般的に契約（および特に契約の電子表現体）の最終的な望ましい特徴は、契約が不履行不能な形態で正確に記録されることである。従来では、これは、関係するすべてのパーティの権利、制約および義務を記載する書面による書類（契約）を作成することを包含する。この書類は読まれ、すべてのパーティによって契約の正確な表現体であるとして署名される。電子契約は、その性質上、最初は書面で提出されない。VDEにより、このような契約が正確に電子的に記述され次に不履行を防ぐために電子的に署名されることが可能である。さらに、この好適な実施態様では、電子契約の条件を人間可読に記述することができるメカニズムが提供される。

VDEは、VDEサイトが解釈可能な制御セットを特定するための簡潔なメカニズムを提供する。機械が解釈可能なメカニズムは人間可読でないことが多い。VDEは、少なくとも一人の人間のユーザの代わりにネゴシエーションプロセスを操作することが多い。従って、ネゴシエーションは「人間可読フォーム」で表現されることが望ましい。オブジェクト、メソッドおよびロードモジュールのためのVDEデータ構造はすべて、それらの構造内に１つ以上のDTDを特定する条項を有する。これらのDTDは項目の一部として格納されるか、または独立して格納され得る

。DTDは、この項目の機能の自然言語による記述を含み得る１つ以上のデータエレメント（MDE、UDEまたは他の関連データエレメント）を記述する。これらの自然言語による記述は、各項目に対して言語独立型の人間可読の記述を提供する。項目の集合体（例えばBUDGETメソッド）は、その機能を記述し電子的に特定され実施可能な契約の条件を形成する自然言語によるテキストと関係付けることができる。条件の集合体（制御セット）は特定の権利に関係する契約を定義する。従って、VDEは、人間が理解し遵守することができる電子契約の電子的な特定化、ネゴシエーションおよび実施を可能にする。

VDE 100は、以下に述べるようにして電子契約のネゴシエーションおよび実施を可能にする。

・ネゴシエーションのための共通のボキャブラリおよび手順を許す権利および制御情報の簡潔な特定化を可能にする。

・ネゴシエーションを行うための安全な処理環境を提供する。

・権利および制御の特定化が確実に配分され得る配分環境を提供する。

・ネゴシエートされた契約が、契約をネゴシエートするプロセスによって電子的に受け取られ署名される安全な処理環境を提供する。

・ネゴシエートされた電子契約を確実に実施するメカニズムを提供する。

ネゴシエーションのタイプ

ネゴシエーションの１つの簡単な形態は、１つのパーティが「コヒーレント」契約を形成するように要請することである。ネゴシエーションにおいて他方のパーティによって選択され得るオプションはあるとしてもほとんどない。要請の受け取り側には１つのオプションしかない。すなわち、要請の中の条件（制御情報）を受け入れるか拒絶するかである。条件を受け入れる場合は、特定化された制御情報という条件付きの権利が与えられる。条件を拒絶する場合は、権利は与えられない。PERCおよびURTの構造は要請によるネゴシエーションをサポートし得る。すなわち、PERCまたはPERCからの制御セットが要請として提示され、受け取り側は要請を受け入れるかまたは拒絶し得る（許可されたメソッドオプションが提示される場合はこれから選択する）。

今日のこのタイプのネゴシエーションの一般的な例は、「シュリンク包装ライセンス」という条件下でのソフトウェアの購入である。多くの広く出回っている電子配布メソッドはこのタイプのネゴシエーションを使用している。CompuServeは同じメソッドで動作するオンラインサービスの一例である。選択は簡単である。すなわち、特定の料金を支払うか、サービスまたはソフトウェアを使用しないかのいずれかである。VDEは、権利および制御情報を記述するPERCおよびURTを提供する能力により、およびコンテンツ所有者が、ユーザが所定のメソッドオプションセットから選択するのを可能にするREGISTERメソッドを提供するのを可能にすることによって、このタイプのネゴシエーションをサポートする。このシナリオでは、REGISTERメソッドは簡単なネゴシエーションプロセスである構成要素を含み得る。

ネゴシエーションのもっと複雑な形態は「押し問答(haggling)」に類似するものである。このシナリオでは、条件のほとんどは固定されるが、一つ以上の条件（例えば価格または支払い条件）は固定されない。これらの条件に対しては、オプション、制限、およびネゴシエーションの余地があるエレメントが存在する。所望の、許可された、および選択可能な条件を決定するために、２つのパーティ間のVDE電子ネゴシエーションが用いられ得る。電子ネゴシエーションの結果が、完成した電子契約を特定する規則および制御情報の最終セットであり得る。１つの簡単な例は、購入者が支払いメソッド（VISA、MasterCardまたはAmerical Express）を選択する能力が加わった上記のソフトウェアを購入するシナリオである。もっと複雑な例は、支払われる価格が使用監査追跡に沿って戻されるユーザについての情報量に依存する購入情報のシナリオである。この第２の例では、コンテ

ンツを使用する権利は２つの制御セットに関係し得る。１つの制御セットは、コンテンツの使用に対して固定（「より高い」）価格を記述し得る。別の制御セットは、制御情報の追加およびユーザの個人情報の収集および返却を必要とするフィールド仕様を伴ったコンテンツの使用に対して固定（「より低い」）価格を記述し得る。これらの場合の両方で、PERCの選択可能で許可されたフィールドおよ

び制御セットは、ネゴシエーションの一部として選択され得るオプションを記述し得る。ネゴシエーションを行うためには、一方のパーティは、PERCによって特定される特定のフィールド、制御情報および制限を含む制御セットを提案する。他方のパーティは、提案された制御セットから取り出して受け入れるか、これらを拒絶するか、または使用され得る代替の制御セットを提案する。ネゴシエーションプロセスは、PERCの許可され、必要とされ、選択可能な指定を使用して、最終的な規則セットのための受け入れ可能なパラメータ領域を決定し得る。同意に達すると、ネゴシエーションプロセスは、ネゴシエーションの結果を記述する新しいPERCおよび／またはURTを作成し得る。得られるPERCおよび／またはURTは、後日の契約の不履行を防ぐために、ネゴシエーションに係わったネゴシエーションプロセスのすべてによって（例えばディジタル署名を用いて）「署名」され得る。

ネゴシエートされるエレメントのさらに他の例としては、電子キャッシュ、注文書、購入証明書（贈与証明書、クーポン）、入札および仕様書、予算「引き下げ(rollbacks)」および調停、通貨為替レート、株購入、ならびに課金レート(billing rate)がある。

上述の第２の例をサポートするために用いられるPERCセットを図75A（コンテンツ所有者によって送られるPERC）、図75B（ユーザの選択および権利を提示するためにユーザによって作成されるPERC）、および図75C（ネゴシエーションプロセスを制御するためのPERC）に示す。

これらのPERCは、このセクションで後述するネゴシエーションプロセスおよびプロトコルのいずれかと共に用いられ得る。

図75Aは、自らの権利のオプションを記述するためにコンテンツ提供者によって作成され得るPERC 3100の一例を示す。この例では、PERCは１つのUSE権利に関する情報を含む。２つの択一の制御セット3102a、3102bがこの例での権利のために提示される。制御セット3102aは、ユーザについての情報を戻さなくてもコンテンツの使用を許可し、もう１つの制御セット3102bは、コンテンツの使用を許可すると共にユーザからの「レスポンスカード」タイプの情報を回収する。制御

セット3102a、3102bの両方とも制御情報のほとんどに対して共通のメソッドセットを用い得る。この共通の制御情報はCSR 3104およびCSO 3106によって表される。

このPERC 3100の制御セット3102aは、コンテンツ提供者にユーザについての情報を提供せずにユーザがコンテンツを使用し得るメカニズムを示している。この制御セット3102aは周知の販売制御メソッドならびに必要なメソッドおよびメソッドオプションセットを特定している。詳しくは、この例では、制御セット3102aはBUDGETメソッド3108（例えばVISA、MasterCardまたはAmerican Express）を定義し、また料金を特定するBILLINGメソッド3110（例えば一回の料金が$100.00）を定義している。

このPERC 3100の制御セット3102bは、ユーザがコンテンツを得る別のメカニズムを示している。この例では、制御セット3102bは異なる販売制御メソッドならびに必要なメソッドおよびメソッドオプションセットを特定している。この第2の制御セット3102bはBUDGETメソッド3116（例えばVISA、MasterCardまたはAmerican Express）、料金を特定するBILLINGメソッド3110（例えば一回の料金がもっと低い$25.00）、ならびに所望され且つ必要なフィールドセットを特定するAUDITメソッド3114を特定している。必要で且つ所望のフィールド仕様3116はDTD仕様の形態をとり得る。ここでは、例えば、フィールド名がリストされる。

コンテンツ作成者は2つの制御セットのうちの一方（例えば制御セット2）を他方より「優先」させる。この場合、ネゴシエーションプロセスでは先ず「優先」された制御セットが「提案」され、ネゴシエーションの他方のパーティがこの「優先」された制御セットを「拒絶」する場合は、これは引っ込められ「非優先」の制御セットに替えられる。

この例では、これら2つの制御セット3102a、3102bは共通のBUDGETメソッド仕様を共有し得る。BUDGETメソッド仕様は、所望であれば、CSR 3104またはCSO 3106の制御セットに含まれ得る。制御セット3102a（情報を戻さずに使用）を選択すると、PERC 3100によって特定されるような固有の構成要素アセンブリが組み立てられる。詳しくは、この例では、「販売」CONTROLメソッド3118、$100の固

定料金のBILLINGメソッド3110、およびCSR 3104およびCSO 3106によって特定される制御情報の残りが選択される。また、ユーザは（例えばVISA、MasterCardおよびAmerican Expressからの）受け入れ可能なBUDGETメソッドの選択を特定する必要がある。制御セット3102bを選択することにより、「レスポンスカードによる販売」CONTROLメソッド3120、BILLINGメソッド3116（例えば＄25の固定料金）、および必要なフィールドDTD 3116にリストされるフィールドを必要とするAUDITメソッド3114を用いる異なる構成要素アセンブリが組み立てられる。プロセスはまた、所望のフィールドDTD3116にリストされるフィールドのうち利用可能なすべてのフィールドを選択し得る。制御情報の残りは、CSR 3104およびCSO 3106によって特定される。制御セット3102bを選択する場合も、ユーザは（例えばVISA、MasterCardおよびAmerican Expressを含むリストからの）受け入れ可能なBUDGETメソッドの選択を特定する必要がある。

図75Bは、ネゴシエーションプロセスでユーザの所望および要件を特定するためにユーザによって用いられ得る制御セット3125の例を示す。この制御セットは、集合されたCSR予算仕様3129およびコンテンツの使用のための２つの制御セット3131a、3131bを含むUSE権利セクション3127を有する。制御セット3131aは、特定のCONTROLメソッド3133およびAUDITメソッド3135の使用を必要とする。特定されたAUDITメソッド3135は、監査追跡で放出され得るフィールド3137のリストによりパラメータ化される。制御セット3131aはまた、一定の金額（例えば＄30.00）を超えない費用とし得るBILLINGメソッド3139を特定し得る。この例の制御セット3131bは、特定のCONTROLメソッド3141を記述し、このオプションが選択される場合は、一定の金額（例えば＄150.00）を超えない費用とし得るBILLINGメソッド3143を参考として示し得る。

図75Eは、上述のネゴシエーションプロセスの「結果」として形成される電子契約3200のより高レベルの図を示す。電子契約3200は多数の条項3202および多数のディジタル署名3204を含み得る。各条項3202は、上記に述べられ図75Dに示される項目3160などのPERC／URTを含み得る。従って、電子契約3200の各「条項」3202は、VDE電子機器600によって組み立てられ実行され得る構成要素アセンブリ6

90に対応する。通常の契約のように、電子契約3200には「パーティ」間の「同意」を具体化するのに必要なだけの契約条項3202が存在し得る。条項3202のそれぞれは電子的にネゴシエートされたものであり、従ってパーティ間の「同意」（例えば「折衷」）の一部を具体化し得る。電子契約3200は、機械、すなわち様々な電子条項3202によって特定されるような構成要素アセンブリ690を組み立てるVDE電子機器600によって文字通り実行され得るという意味で、「自己実行」的である。電子契約3200は、構成要素アセンブリ690と共に使用される上述の同じVDEメカニズムを用いて自動的に「実施」される。例えば、条項3202(2)が支払いまたはBILLING条件に対応すると仮定すると、その対応する構成要素アセンブリ690は、ユーザのVDE電子機器600によって組み立てられると、支払い条件が正しいかどうかを自動的に決定し、正しいときは、適切な支払いメカニズム（例えばユーザに対する仮想「クレジットカード」オブジェクト）に自動的にアクセスして、その支払いが行われるように調整する。別の例としては、電子契約条項N3202(N)が特定のVDE参加者に監査情報を提供するユーザの義務に対応すると仮定すると、電子契約3200によって、VDE電子機器600は、例えば、安全データベース610内の適切な監査追跡にアクセスし、管理オブジェクト内の監査追跡を正しい参加者に提供し得る対応する構成要素アセンブリ690を組み立てる。図75Fは、条項3202(N)が、例えば、取引3206に多数のステップが生じるように調整する構成要素アセンブリ690を特定し得ることを示す。このようなステップのいくつか（例えばステップ3208(4)、3208(5)）は、例えば、コンテンツ使用が一定の量を超えているかどうか、一定の期間が過ぎたかどうか、一定のカレンダー日に達したかどうかなどの試験において条件付きであり得る（例えば3208(3)）。

図75Eの電子契約に示すディジタル署名3204は、例えば、上述のような公開鍵技術を用いる従来のディジタル署名を含み得る。電子契約3200の中にはディジタル署名3204を含まないものもある。しかし、電子契約3200のパーティであるユーザの電子機器600に電子契約にディジタル署名するよう要求して、ユーザが証拠となる目的のために後で契約の履行を拒むことができないようにするようにすることが望ましい。同じ契約に多数のパーティが存在する場合は、書面による書類

に記録された契約の多数のパーティがインクペンを用いて書類に署名するのと同様に、同じ電子契約3200にそれぞれがディジタル「署名」し得る。

電子契約3200の条項3202のそれぞれは、最終的には、PPE 650によって実行され得るデータおよびコードの集合体に対応し得るが、場合によっては、電子契約の人間可読バージョンを提供する必要があり得る。この必要は、上述のように、契約を「自己実行」するために用いられる構成要素アセンブリ690に関係する1つ以上のDTD内にテキストを提供することによって実現され得る。このようなテキストは、例えば、対応する電子契約条項3202が何を意味または包含するかを機能的観点から記述し、および／または契約の下での法的義務が何であるかまたは何を表しているかを法的に実施可能な用語で記載し得る。このようなテキストをテキストライブラリから供給するために「テンプレート」（本明細書のどこかに記載）が用いられ得る。異なるテキストエレメントを結合してコヒーレントで人間可読の契約書類にまとめるシンタックス規則を確立するために、エキスパートシステムおよび／または人工頭脳能力が用いられ得る。このようなテキストは、必要であれば、「人間」の代理人によって検討および改変されて、パーティ間の特定の契約のためにこれをカスタマイズし、および／または内部で具体化され、VDE電子機器600で実行する関係する構成要素アセンブリ690によって実施される「自己実行」電子義務を増やして法的義務をさらにつけ加えることができる。このようなテキストは、電子契約の実行により自動的にまたは要請があり次第表示され得るか、または契約の印刷された人間可読バージョンを生成するためにいつでも使用され得る。電子契約3200のこのような書類バージョンは、（望まない場合は）契約のパーティによってインクで署名される必要はない。なぜなら、ディジタル署名3204が、契約のすべての条件へのパーティの相互の同意を提供する十分に安全で信頼のある証拠となる基礎を提供するからである。

この好適な実施態様では、ネゴシエーションプロセスは、プロセスを特定する別のPERCの指示の下でPPE 650内で実行される。図75Cは、ネゴシエーションプロセスを特定するPERC 3150の一例を示す。PERC 3150は、ネゴシエーションのための単一の権利3152、およびこの権利のための２つの許可された制御セット3154a、3154bを有する。第１の制御セット3154aは「信頼されたネゴシエーション」の

た

めに用いられ得る。すなわち、これは、所望のネゴシエーションCONTROLメソッド（「ネゴシエーション」）を参考として示し、このCONTROLメソッドが用いる２つのUDEを（フィールド3157a、3157bで）参考として示してる。これらのUDEは、例えば、図75Aおよび図75Bに示されるPERC3100、3125であり得る。第２の制御セット3154bは、ネゴシエーションを管理するために「多ネゴシエーション」プロセスによって用いられ得、２つのネゴシエーションメソッド、「ネゴシエーション１」および「ネゴシエーション２」を提供し得る。両方のネゴシエーションプロセスは、それぞれPERC3100、3125を入力とする必要なメソッド（「ネゴシエーション１」および「ネゴシエーション２」）3156、3158として記述され得る。この例のこの制御セットのためのCONTROLメソッド3158は、２つのネゴシエーションプロセスが互いに通信するために用いるサービスの名前を特定し得、またネゴシエーションから得られるURTの作成を管理し得る。

図75Cに示すPERC3150によって特定されるネゴシエーションプロセスが実行されるときは、このプロセスには、ネゴシエーションのための基礎として用いられ得る入力としてPERC3100、3125が配備され得る。この例では、ネゴシエーションプロセスのタイプ（信頼されたネゴシエーションまたは多ネゴシエーション）の選択は、VDEノードを実行することによって行われ得る。図75Cに示すPERC 3150は、例えば、ユーザからの登録要求に応答してRESISTERメソッドによって作成され得る。このPERC3150によって特定されるプロセスは、次にRESISTERメソッドによって用いられ、これにより電子契約の条件のネゴシエーションが開始され得る。

この例のネゴシエーションプロセスの間、図75Aおよび図75Bに示すPERC 3100、3125は、図75Cに示すPERC 3150に基づいて作成された構成要素アセンブリによって比較される入力データ構造として働く。制御セットによって特定される構成要素アセンブリは、ネゴシエーションの進行と共に、組み立てられそして比較され、必要な「条件」から始まって、好適な／所望の「条件」に進み、次に許可された「条件」へと移動する。メソッドオプションの選択は、PERC 3100、3125に

特定された所望のメソッドおよびメソッドオプションを用いて行われる。この例では、図75Aに示すPERC 3100のための制御セットは、図75Bに示すPERC 3125と比較され得る。「一致」するとネゴシエーションは成功裏に完了し、「結果」が生成され

る。

この実施態様では、このようなネゴシエーションの結果は通常はURTとして書かれ、同意に達したことを示すためにネゴシエーションプロセスによって「署名」され得る。これらの電子署名は、（仮想の）「心の会合（meeting of minds）」に達した（契約が存在するための従来の法的前提条件の１つ）ことを示す手段を提供する。上記の例によって作成されたはずのURT 3160の一例を図75Dに示す。このURT 3160（これ自体PERC 808であり得る）は、ネゴシエーションで「同意された」「条件」を反映する制御セット3162を含む。この例では、「同意された」条件は、これらのPERCによって必要とされる条件と「同じ位に有利」でなければならないという意味で、入力されたPERC 3100、3125によって必要とされる条件と「一致」しなければならない。示されたネゴシエーション結果は、例えば、ある意味では図75AのPERC 3100の制御セット3102aおよび図75Bの制御セット3131aに対応する「ネゴシエートされた」制御セット3162を含む。従って、得られる「ネゴシエートされた」制御セット3162は、必要とされるAUDITメソッド3166を含み、このメソッドは、制御セット3125の所望のBUDGETメソッド3142に対応するが、制御セット3100が必要とするBUDGETメソッド3112によって許容される制御セット範囲「内」である必要なBUDGETメソッド3164含む。同様に、得られるネゴシエートされた制御セット3162は、必要とされるAUDITメソッド3166を含み、このメソッドは、PERC 3100が必要とするAUDITメソッド3114およびPERC 3125が必要とするAUDITメソッド3135の両方の要件に従う。同様に、得られるネゴシエートされた制御セット3162は、必要とされるBILLINGメソッド3170を含み、このメソッドは、PERC 3100が必要とするBILLINGメソッド3116およびPERC3125が必要とするBILLINGメソッド3170のそれぞれに「一致」するまたはこれに従う。

別のクラスのネゴシエーションとして、規則は固定されず所望の目標のみが特

定されるものがある。このタイプのネゴシエーションのためのネゴシエーションプロセスは非常に複雑となり得る。これは、人工頭脳、ファジー論理、および／または目標に到達するための関連アルゴリズムを利用し得る。VDEは、権利、制御情報、フィールドおよび目標を（所望の権利、制御情報およびフィールドの形態で）簡潔に特定するメカニズムを提供することによってこれらのタイプのプロセスをサポートする。これらのタイプのプロセスのための目標は、オプションの、許可された、または所望のエレメントと名付けられる特定のエレメントを含む１つ以上の制御セットとして特定され得る。

ネゴシエーションのタイプ

この好適な実施態様におけるネゴシエーションは以下のいずれかで構築され得る。

１．共有知識

２．信頼されるネゴシエータ

３．「ゼロベース」の知識

「共有知識」ネゴシエーションは、ネゴシエーションに関係する規則および規制のすべてをすべてのパーティが知っていることに基づく。要請によるネゴシエーションは共有知識によるネゴシエーションの簡単な例である。要請者は、まとめて受け入れられるかまたは拒絶される要請リストを提示する。要請リストは、リストの各項目を受け入れるかまたは拒絶するために必要な完全な知識セットを備えている。VDEは、要請を符号化し、確実に通過させ、そしてVDE安全処理および通信能力を用いる安全なVDE下位システム間でおよびこれらにより確実に処理され得るメカニズムを提供することによって、このクラスのネゴシエーションが電子的に行われるのを可能にする。VDEによって用いられる別のタイプの共有知識によるネゴシエーションは、２つ以上のネゴシエーションパーティ間の情報の交換を含む。すなわち、ネゴシエーションプロセスは、所望の最終出費を個々のプロパティに基づいて個別に決定する。次にプロセスはこれらの間に相違があればこれをネゴシエートし得る。共有知識によるネゴシエーションは（要請タイプのネゴシエーションにおけるように）１つのネゴシエーションプロセスしか必要

としないか、または２つ以上の協働プロセスを含み得る。図76Aおよび図76Bは、共有知識によるネゴシエーションで２つのネゴシエーションプロセスが使用される場合のシナリオを示す。

図76Aは、（例えば、異なるパーティによって供給される）PERC 808をいくつでもネゴシエーションへの入力とする単一のネゴシエーションプロセス3172を示す。ネゴシエーションプロセス3172は、別のPERC（例えば図75Cに示されるPERC 3150）によって供給され得る「ネゴシエーションプルセス規則および制御情報」の監督下でVDEノードで実行される。プロセス3172は、ネゴシエーションの結果として１つ以上のPERC／URT 3160を生成する。

図76Bは、それぞれが１つのパーティからのPERC 808およびネゴシエーションプロセスを制御する別のPERC 3150を入力とし、またそれぞれがネゴシエートされた「結果」であるPERC／URT 3160を出力として生成する多数のネゴシエーションプロセス3172A～3172Nを示す。プロセス3172A～3172Nは、同じまたは異なるVDEで実行し得、また「ネゴシエーションプロトコル」を用いて通信し得る。

単一のおよび多数のネゴシエーションプロセスは特定のVDEサイトのために使用され得る。ネゴシエーションプロセスは名称を持ち、周知のメソッド名を用いてアクセスすることができる。PERCおよびURTは、ネゴシエーションを制御する制御PERCおよびREGISTERメソッドのように、サイトでの処理のために管理またはスマートオブジェクトにおいて遠隔VDEサイトに伝送され得る。

多ネゴシエーションプロセスは、物理的に離れたVDEサイトに存在する安全プロセス（安全下位システム）間の安全な通信を含む、これらのプロセス3172間で通信する能力を必要とする。VDEは、プロセス間通信を、構成により必要であれば使用され得る確実に提供されるサービスに一般化する。プロセス間通信はネゴシエーションプロトコルを用いて規則セットについての情報をプロセス3172間で交換する。ネゴシエーションプロトコルの１つの例は以下のネゴシエーション「原始関数」を含む。

WANT　　条件セットを望む

ACCEPT　　条件セットを受け入れる

REJECT　　条件セットを拒絶する

OFFER　　条件セットの代わりに他の条件セットを提案する

HAVE　　条件セットが可能であるかまたは望ましいと主張する

QUIT　　同意に達することなくネゴシエーションの終了を主張する

AGREEMENT　ネゴシエーションを終了し署名のために規則セットを通過させる

WANT原始関数は、権利および制御セット（または制御セットの一部）の情報を取り出し、特定の条件が所望されるかまたは必要であることを他のプロセス3172に主張する。要請によるネゴシエーションは、WANT原始関数が要請を主張するために用いられる簡単な例である。この例のプロトコルは、WANT原始関数の洗練された形態であるREQUIREを導入し得る。この例では、REQUIREは、１つのパーティが契約を形成するために必要であると決定する条件をそのパーティが設定するのを可能にする。一方、WANTは、所望であるが必須ではない条件をパーティが設定するのを可能にする。これにより、「持たなければならない」と「持ちたい」とが区分され得る。

この例では、WANT原始関数はいつでも、ACCEPT、REJECTまたはOFFER原始関数によって返答されなければならない。ACCEPT原始関数は、ネゴシエーションプロセス3172が条件セットを受け入れるのを可能にする。REJECT原始関数は、プロセス3172が提案された条件セットを拒絶することを可能にする。必要な条件セットを拒絶するとネゴシエーションは終了する。OFFERは対案の提出を可能にする。

HAVE、QUITおよびAGREEMENT原始関数は、ネゴシエーションプロトコルが規則セットについての情報を通過させるのを可能にする。共有知識によるネゴシエーションは、例えば、すべてのネゴシエーションプロセス3172A～3172Nが（私のPERCを）HAVEすることを他のプロセスに主張することで開始される。HAVEはまた手詰まり状態になったときに使用され、一方のプロセス3172が他方のプロセス3172に許可されたオプションについて知らせる必要がある。QUITは、同意に達しないでネゴシエーションが不成功に終了することを示す。AGREEMENTは、同意が成功したことを示し、得られる「ネゴシエートされた」PERC／URT 3160を署名のために他のプロセス3172に渡す。

「信頼されたネゴシエータ」ネゴシエーションでは、すべてのパーティがそれぞれの要請および好みを「信頼された」ネゴシエータに提供し、ネゴシエータの決定に拘束されることに同意する。これは今日の社会での拘束力のある仲裁に類似する。VDEは、「信頼された」ネゴシエーションサービスが形成され得る環境を提供することによってこのネゴシエーションモードを可能にする。VDEは、要請、所望および制限を（例えばPERCに）簡潔に特定し得るメカニズムだけではなく、PERCが、ネゴシエーションが如何に行われるかを特定する規則セットと共に

「信頼された」ネゴシエーションサービスに確実に転送されるメカニズムを提供する。このネゴシエーションモードはまた、ネゴシエーションプロセスが不正改変されないように安全な実行環境を提供することによって可能となる。信頼されたネゴシエータサービスは、サイトの完全性が周知であるVDEサイトで用いられ得る。信頼された遠隔ネゴシエーションサービスは、１つ以上のネゴシエーションプロセスを実行するのに十分な計算資源を所有しないVDEサイトによって使用され得る。すなわち、このサービスを提供しこのサービスが代わってネゴシエーションを扱うのを可能にするVDEサイトへの通信リンクを確立し得る。

「ゼロベース」知識のよるネゴシエーションは、認証のために用いられるゼロベース知識プロトコルのいくつかの特徴を共有する。遠隔サイトが特定の項目の保持者であるかどうかをその項目が交換も曝露もされなくても決定し得るプロトコルを構築するメソッドは当該分野では十分理解される。このタイプのプロトコルは、制御セットをその知識ベースとして使用する少なくとも１つのVDEサイトで作動する２つのネゴシエーションプロセス間で構築され得る。ネゴシエーションプロセスは、それらの制御セットについての情報を交換し得、それらの個別の規則セットを用いることに関しての要請および対案を作成し得る。例えば、ネゴシエーションプロセスＡはネゴシエーションプロセスＢと通信してある本を読む権利をネゴシエートする。ネゴシエーションプロセスＡは本を読む権利に対して＄10.00を超えない金額を支払い、この権利に対して＄5.00から＄6.00の間の金額を支払うのが好ましいと特定する。プロセスＡの規則セットはまた、＄5.00オプションに対しては読者の氏名および住所の放出を認めると特定する。プロセス

Ｂの規則セットは、その本を読む権利に対して＄５０.００の支払いを望み、ユーザが自分自身についての情報を放出することに同意するならば＄５.５０で本を提供すると特定する。ネゴシエーションは以下のように進み得る。

プロセスＡ　　<--> プロセスＢ

ＷＡＮＴ（読む権利、非制限）　　-->

<--　ＨＡＶＥ（読む権利、非制限、＄５０）

ＯＦＦＥＲ（読む権利、ユーザ情報を提供）　-->

<--　ＨＡＶＥ（読む権利、ユーザ情報を提供、＄５.５０）

ＡＣＣＥＰＴ（読む権利、ユーザ情報を提供、＄５.５０）　-->

上記の例では、プロセスＡは、制限または他の情報放出はなしに本を読む権利を所望すると特定する。この開始位置は、プロセスＡが規則として用いるＰＥＲＣの権利オプションとして特定される。プロセスＢはこの規則をチェックして、非制限の読む権利は実際には＄５０の価格で許可されると決定する。プロセスＢは、この条件が利用可能であるとプロセスＡに返答する。プロセスＡはこの返答を受け取り、プロセスＡが規則ベースとして用いるＰＥＲＣ内の制御セットに対してこれをチェックする。＄５０はこの規則セットに対して特定された＄１０の制限から外れるため、プロセスＡはこの提案を受け入れることはできない。プロセスＡは、非制限の読む権利を読者の名前および住所の放出と組み合わせた（別の選択可能権利オプションで述べたような）対案を作成する。名前および住所フィールドはプロセスＡのＰＥＲＣが参考とするＤＴＤに記述されている。プロセスＢはＰＥＲＣのその規則をチェックし、個人情報の放出と組み合わせた非制限の読む権利が許可されたオプションであると決定する。プロセスＢは、プロセスＡによって提供されるＤＴＤに記述されている放出される予定のフィールドを、それ事態のＰＥＲＣのＤＴＤの所望のフィールドと比較し、受け入れ可能な一致があったと決定する。プロセスＢは次に特定情報の放出を伴う非制限の権利を＄５.５０で許可する提案をプロセスＡに送る。プロセスＡは、権利、制約およびフィールドをその規則セットと比較し、

＄５.５０がその規則セットに受け入れ可能であると記載されている＄５～＄６の範囲内であると決定する。プロセスＡはこの提案をそのまま受け入れる。この提案は両パーティが、最終ネゴシエーションの結果（非制限権利、ユーザ情報の放出、＄５.５０）を記述する新しいPERCに「署名」することによって封印される。新しいPERCは、プロセスＡの所有者によって、記述された条件に従ってコンテンツ（本）サブジェクトを読むために利用され得る。

別の取り扱いモデルチェーン

図２に関連して述べたように、例えばコンテンツ配布のために使用されるVDE取り扱いおよび制御チェーンの１つの例では、VDE １００の４つの「参加者」事例がある。これらの参加者事例の第１はコンテンツ作成者１０２であり、出版者、作家、権利所有者、または消費者への配布のために情報を準備する著作権の配布者によって操作される。第２の参加者事例はVDE権利配布者１０６であり、権利を配布しまたVDE承認情報の消費者の使用を管理および分析し得る。第３の参加者事例はコンテンツユーザ１１２であり、ユーザが情報を使用するときユーザ（最終ユーザおよび配布者を含む）によって操作される。第４の参加者事例は金融情報交換所１１６であり、VDE関連の情報交換所活動を可能にする。さらに別の参加者、VDE管理者は、VDE １００を適切に作動させ続けるためのサポートを提供し得る。適切な承認およびインストールされた権利作動システム（Rights Operating System）の構成要素により、いかなるVDE電子機器６００でもこれら参加者の役割のいずれかまたはすべてを演じることができる。

著作権はVDE １００にとって原料の１つの例である。この原料を最終商品に転換するために、出版者、作家または権利所有者は、ディジタル情報（電子ブック、データベース、コンピュータソフトウェアおよび映画など）を「オブジェクト」と呼ばれる保護されたディジタルパッケージに変換するツールを使用する。配布者１０６からパーミッションを受ける消費者（または再配布者などの所有チェーンに沿った他の者）のみがこれらのパッケージを開けることができる。VDEのパッケージ化されたコンテンツは、コンテンツ作成者１０２および／またはコンテンツ配布者１０６によって、またはコンテンツの配布通路の他のVDE参加者、すなわち、

通常は、制約される参加者ではなくVDE安全パッケージの作成に「より近い」参加者によって提供される「規則および制御情報」によって束縛され得る。

コンテンツが「オブジェクト」にパッケージ化されると、ディジタル配布プロセスが開始され得る。情報パッケージ自体は保護されているので、CD-ROMディスクでまたはコンピュータネットワークを介して自由に配布され得、もしくはケーブルを介してまたは放送波により放送され得る。保護されたパッケージの最終ユーザ間の非公式の「チャネル外」交換はコンテンツの所有権にとって危険とはならない。なぜなら、承認された個人のみがこれらのパッケージを使用し得るからである。実際には、このような「チャネル外」の配布は、マーケット浸透の限界原価メソッドとしていくつかのコンテンツ提供者によって奨励されている。使用の承認（例えば、一定のドル使用額を許すVISA情報交換所予費）を得ている消費者は、例えば隣人によって提供されるチャネル外のVDE保護パッケージのライセンスを自由に得ることができる。

最終ユーザは、VDEパッケージを開けてそのコンテンツを利用するためにはパーミッションを得なければならない。配布者106はこのようなパーミッションを与えることができ、また（上位の制御情報によって許可される場合は）非常に柔軟にパッケージコンテンツを使用するメソッドに制限を加えるかさもなくばこれを特定することができる。配布者106および金融情報交換所116はまた、典型的には、金融責任を持つ（これらは、所望であれば、ある環境下では同じ組織であり得る）。これらは、最終ユーザからの必要な支払いがこれら自体のおよび他の参加者の要件を満たすことを確実にする。これは監査の使用によって実現される。

VDE 100を使用する配布者106は、ソフトウェア出版者、データベース出版者、ケーブル、テレビおよびラジオ放送者、ならびに他の電子形態での情報配布者を含み得る。VDE 100は、放送または遠隔通信による、または電子記憶媒体の物理的な転送による配布を含む、すべての形態の電子配布をサポートする。また、パーミッション、制御メカニズムおよびコンテンツの個別の配送による多数の配布タイプからの情報を途切れなく統合する、均質な形態でのコンテンツの配送もサポートする。

配布者106および金融情報交換所116はそれら自体が、それらの管理活動の安全な記録に基づいて監査され得、信頼性の高い「信頼された」プロセスチェーンにより、ディジタル配布プロセス全体の完全性が確実となる。これにより、コンテンツ所有者が、例えば、かれらが実際のコンテンツ使用または他の同意された基本に基づいて適切な補償を受けていることを検証することが可能となる。

最終ユーザ112はこの例ではコンテンツの最終消費者であるため、VDE 100は、最終ユーザが受け取ったパーミッションの制限内にいる限り、保護されたコンテンツを途切れのない透明なメソッドで提供するように設計されている。最終ユーザ112の活動は、配布者106によって監査を行うことができるように計量され得る。監査プロセスはユーザのプライバシの懸念を満足させるようにフィルタリングお

よび／または一般化され得る。例えば、計量され記録されたVDEコンテンツおよび／または機器使用情報は、配布者106への報告の前にフィルタリングされ、これにより、コンテンツ使用者112および／またはその使用についての必要以上の情報が曝露されないようにし得る。

VDE 100は、コンテンツ提供者に、それらの従来の配布戦略の重要な局面を電子形態に作成し直し、それらの個々の必要性および環境にとって適切な新しい配布メカニズムを革新的に構築する能力を与える。VDE 100は配布チェーン内の関連する参加者をサポートし、また所望の価格戦略、アクセスおよび再配布パーミッション、使用規則、ならびに関連する管理および分析手順を可能にする。VDE 100の再使用可能な機能的原始関数は、コンテンツ提供者によって柔軟に組み合わされて、それぞれの配布目的を反映させることができる。この結果、コンテンツ提供者は、情報を確立された配布チャネルの供給し、また自らの個人化された配布チャネルを作成することができる。

仮想配布環境100の様々な参加者の役割の概要を以下の表に示す。

役割	記述
「従来の」参加者	
コンテンツ作成者	ディジタル情報のパッケージ作成者および最初の配布者
コンテンツ所有者	ディジタル情報の所有者
配布者	予算および／またはコンテンツのための権利配布サービスを提供
監査人	使用に基づいた監査追跡を処理および減らすサービスを提供
情報交換所	コンテンツおよび監査情報のための中間格納および転送サービスを提供。また、典型的には、第三者金融提供者および監査人を含む他のサービスのための基準を提供
ネットワーク提供者	サイトと他の参加者との間の通信サービスを提供
金融提供者	最終ユーザおよび配布者への電子資金の第三者源の提供者
最終ユーザ	情報の消費者
他の参加者	
再配布者	コンテンツ提供者および／または他の配布者からの制約を扱うチェーンに基づいてコンテンツを使用する権利を再配布
VDE管理者	VDEノードをサポートするための信頼されたサービスの提供者
個別の監査処理者	監査追跡データを処理および要約化するサービスの提供者。コンテンツ提供者が必要とする分かりやすい監査能力を維持する一方で、最終ユーザに匿名性を提供
エージェント	最終ユーザおよび他のVDE参加者に対して配布された存在を提供

これらの様々なVDE参加者の中で、「再配布者」、「VDE管理者」、「独立した監査処理者」および「エージェント」は、ある面では、多くの「従来の」ビジネ

スモデルでは対応するもののない「新しい」参加者である。他のVDE参加者（すなわち、コンテンツ提供者、コンテンツ所有者、配布者、監査人、情報交換所、ネットワーク提供者および金融提供者）は、従来の配布モデルは多くの場合仮想配布環境100内で果たすのと同じビジネス上の役割のいくつかを実行する非電子参加者を含むという意味で「従来の」なビジネスモデルの対応するものを有する。

VDE配布者106はまた、電子情報を他の最終ユーザに提供する「最終ユーザ」を含み得る。例えば、図77は、本発明によって提供される仮想配布環境100の取り扱いおよび制御チェーンの別の例を示す。図２に較べて、図77は新しい「クライアント管理者」参加者700を含む。さらに、図77は、すべてがクライアント管理者700の「管轄権」に依存し得る、いくつかの異なるコンテンツユーザ112(1)、112(2)、...、112(n)を示す。クライアント管理者700は、例えば、組織特異的な「規則および制御情報」に依存して、雇用者または他の組織参加者ユニット（課、部、ネットワークおよび／またはグループなど）に権利を配布する企業または他の組織内の別の権利配布者であり得る。クライエント管理者700は、作成者102および／または配布者106によって特定される「規則および制御」に依存して、配布のための規則および制御情報を形成し得る。

上述のように、VDE管理者116bは、VDE 100をサポートし、これが適切に動作するように保持する信頼されたVDEノードである。この例では、VDE管理者116bは、とりわけ、以下のうちのいずれかまたはすべてを提供し得る。

・VDE機器初期化サービス

・VDE機器再初期化／更新サービス

・鍵管理サービス

・「悪党」VDEサイトの「ホットリスト」

・証明書承認サービス

・公開鍵登録

・クライアント参加者ユニットコンテンツ予算および他の承認

VDE 100のすべての参加者は、いかなる役割にも参加する内在的な能力を有す

る。例えば、ユーザは、現在の保護されたパッケージを集め、自らのパッケージを加え（新しいコンテンツを作成し）、そして新しい商品を作成し得る。ユーザは自らの配布者として働くかまたはこの責任を他者に転付するかを選択し得る。これらの能力は、今日市場に入りつつあるオブジェクト志向のパラダイムでは特に重要である。複合オブジェクトの作成、オブジェクトの結合および埋め込み、ならびに他の多源プロセスにより、VDEのこれらの能力に対する必要性が生じている。VDE 100によって提供される配布プロセスは対称性がある。最終ユーザは、再配布を統制している配布チェーンVDE制御情報によって確立された規則からパーミッションを得てこれに従うならば、受け取った情報を他の最終ユーザに再配布し得る。また、最終ユーザは、同じ規則およびパーミッションの制約内で、他者に所有されるコンテンツを新しく発行された作品内に入れ込み、これらの作品を個別に配布し得る。新しい作品のためのロイヤリティの支払いは、出版者、配

布者または最終ユーザによってアクセスされ、追跡され、チェーンのいずれかの段階で電子的に回収され得る。

独立した金融提供者はVDE 100で重要な役割を果たし得る。VDE金融提供者の役割は、従来の配布シナリオにおいてVISAなどの組織が果たす役割と類似している。いかなる配布モデルにおいても、商品またはサービスの使用に対する支払いを承認することおよび使用の一貫性および不規則性を監査することは重要である。VDE 100では、これらは独立した金融提供者によって満たされる役割である。独立した金融提供者はまた、監査サービスをコンテンツ提供者に提供し得る。従って、使用についての予算または制限および監査または使用の記録は、情報交換所116によって処理され得（そして情報交換所によって定位置に配置され得る）。情報交換所は次にユーザ112からの使用の支払いを回収し得る。いかなるVDEユーザ112も、上位の制御情報によって許される程度までは、それらに代わって情報の処理またはサービスの実行を行う権利を与えられ得る。１つのVDE参加者が別のVDE参加者に代わって働くアレンジメントは「代理」と呼ばれる。監査、配布および他の重要な権利は、コンテンツ提供者によって許可されるならば、「代理

」が立てられ得る。「代理」の１つの特別なタイプはVDE管理者116bである。VDE管理者は、VDE電子機器のためのVDE安全下位システム制御情報の一部またはすべてを管理する（例えば「介入」してリセットする）パーミッションを有する（金融情報交換所116としても働き得る）組織である。この管理権は、VDE下部構造に新しい機器を認めること、および「潰された」さもなくば動作不能の機器を改修すること、およびVDEを定期的に更新することのみに拡張され得る。

オブジェクトの作成、配布方法、予算、および監査の更なる説明

好適な実施形態におけるVDEノード電子機器600は、本発明によるオブジェクトの作成、配布、監査収集および使用制御機能を行う能力を有し得る。この範囲の能力を、好適な実施形態によって提供された多くの電子機器600の各々に組み込むことが、インストレーションの統合において、安全な、信頼できる、仮想取引／配布管理環境を構成する、電子取引計量、制御、および課金に対する単一の（または卓越した）標準を作成するという一般的な目標にとって重要である。一般的に考えて、少なくとも汎用VDEノード電子機器600において、ある種のキーとなる機能が概してまたは頻繁になくなるとすると、電子取引／配布管理用の広範囲なアプリケーションを満足させるために、様々な異なるプロダクトおよび異なる標準が出てくる。進化する「電子ハイウェイ」の逼迫した必要性に応答するために、ツールの単一の一貫したセットおよび単一の「合理的な」信頼できるセキュリティおよび商用配布環境を導入する必要はない。ある形態のビデオカセットプレーヤおよびケーブルテレビコンバータなどの、埋め込まれた専用VDEマイクロコントローラを組み込んだVDEノードを含むある種の電子機器600のある種の形態は、必ずしも完全なVDE能力を有していないことがあり得、また必要としないこともあり得る。しかし、好適な実施形態は、多くの分散され離散的に位置する電子機器600を提供する。電子機器600の各々は、オブジェクト著作能力に加えて、著作能力、配布、抽出、監査、および監査リダクション(audit reduction)能力を有することが望ましい。

好適な実施形態によって提供されるVDEオブジェクト著作能力は、著者に、例えば、VDEオブジェクト300に、メソッドを組み込むための様々なメニューを提供

する。メニューは以下を含む、

●VDEオブジェクトのコンテンツ部分の使用がどのように制御されるべきかを規定する計量及び／又は課金メソッド用メニュー、

●VDEオブジェクトのユーザがそのオブジェクトから情報を抽出することを制限する及び／又は可能にする抽出メソッドに関連するメニューであって、このような情報を新しく作成された及び／又は予め存在するVDEコンテンツコンテナ内に入れることを含み得るメニュー、

●監査メソッド、すなわち、ある種の監査情報が生成されて何らかの安全な様式でオブジェクトプロバイダ、オブジェクトクリエータ、管理者、及び／又は情報交換所に通信で戻されるべきかどうかを特定するメニュー、そして、

●オブジェクトがどのように配布されるかを制御するメソッドを配布するメニューであって、例えば、異なる参加者の配布権を、参加者がVDEコンテンツコンテナ取り扱いのチェーンのどこに存在するかによって制御することを含むメソッドを配布するメニュー。

著作能力はまた、管理予算、オブジェクト配布制御鍵、および監査制御鍵を配布者および、著者、配布者及び／又は自分たち自身のために配布及び／又は監査機能を果たすことを承認された他のVDE参加者に配布する手続きを含み得る。著作能力はまた、配布メソッド、監査メソッド、および監査リダクションメソッドを選択および配布する手続きを含み得る。上記メソッドは、例えば、配布者がVDEチェーンの次のコンテンツ取り扱い参加者にオブジェクトを再配布するための予算を安全に書き込む及び／又は制御するメソッドを含む。

著者により作成されたオブジェクト300のコンテンツは、VDE認識アプリケーションプログラムまたは非VDE認識アプリケーションプログラムの援助を得て生成され得る。このようなプログラムとの組み合わせにより著者により作成されたオブジェクトのコンテンツは、テキスト、フォーマットされたテキスト、画像、動画像、音声、コンピュータソフトウェア、マルチメディア、電子ゲーム、電子トレーニングマテリアル、様々なタイプのファイルなどを、何らの制限もなく含み得る。著作プロセスは、著者によって生成されたコンテンツをオブジェクト内に

カプセル化し、１以上の鍵でコンテンツを暗号化し、１以上のメソッドを追加することにより、ユーザ（及び／又は承認されたユーザのみ）によるオブジェクトの許可された使用並びに／又は上記使用に対して必要とされる監査及び／又は支払いのパラメータを規定し得る。著作プロセスはまた、オブジェクトを配布する局面のいくつかまたは全部を含み得る。

一般に、好適な実施形態において、著者は、以下のことをし得る。

Ａ．オブジェクト内にどのコンテンツを含むべきかを特定する。

Ｂ．以下を含むコンテンツベースのメソッドを特定する。

情報--典型的には、コンテンツ及び／又は著者に関する、抽象的な、プロモーション用、識別用、予定作成用、及び／又は他の情報。

コンテンツ--例えば、ファイルリスト及び／又はコンテンツ、時間、変数などを含む他の情報リソース。

Ｃ．制御情報（典型的には、変数を規定するいずれかのメソッドを含む、１以上の許可記録により互いに関連づけられるメソッドのひとまとまり）、および例えば以下を含む初期の承認されたユーザリストを特定する。

アクセスおよび抽出に対する制御情報

配布に対する制御情報

監査処理に対する制御情報

VDEノードが、オブジェクトおよび関連する配布鍵情報を配布するための管理予算情報をオブジェクトプロバイダから受け取る場合、VDEノード電子機器600は、例えば、オブジェクトプロバイダの代わりにオブジェクトを配布し得る。

VDEノードが、いずれかの必要な管理予算、監査メソッド、および（例えば、監査追跡を復号化するために用いられる）監査鍵情報をオブジェクトプロバイダから受け取る場合、VDEノード電子機器600は、オブジェクトプロバイダの代わりに監査記録を受け取り且つ処理し得る。監査能力を有するVDE電子機器600は、監査リダクションメソッドの実行を制御し得る。好適な実施形態における「監査リダクション」は、オブジェクトプロバイダ（例えば、オブジェクトの取り扱いチェーン上のいずれかのオブジェクトプロバイダ）がオブジェクト配布者、オブジ

エクトクリエータ、クライアント管理者、及び／又は監査情報のいずれかの他のユーザに報告されると特定した監査記録及び／又はプロセスから情報を抽出するプロセスである。これは、例えば、ユーザがオブジェクトコンテンツを使用することに対する支払いをすることが必要とされ得る広告者を含み得る。１つの実施形態において、例えば、情報交換所は、予算、監査メソッド、及び／又は監査鍵情報を、ユーザサイトに位置するか、またはオブジェクトプロバイダサイトに位置するオブジェクト、またはオブジェクトのクラス若しくは他のグルーピングに「追加する」能力を有し得る。それにより、所望の監査プロセスが「信頼される」様式で行われることが保証される。VDEコンテンツコンテナ及び／又はコンテンツコンテナ制御情報オブジェクトを取り扱うチェーンの参加者は、オブジェクトコンテンツの使用に関連する使用監査情報を取り扱うチェーン内の別のパーティ（例えば、情報交換所、広告者、または市場調査及び／又は特定の顧客使用情報に関心を持つパーティ）の「プロキシ」として作用し得る。これは、上記他のパーティのために、予算、監査メソッド、及び／又は監査情報が集められ及び／又は適切な様式で上記追加のパーティに提供されることを保証するために必要であり得る鍵情報を特定すること、例えば、上記他のパーティにより提供される仕様情報を採用することにより行われ得る。

オブジェクト作成および初期制御ストラクチャ

VDEの好適な実施形態における、オブジェクト作成および制御ストラクチャ設計プロセスは、制御情報の基本的構成調整可能性(configurabilily)をサポートする。このことは、VDE100が、可能性のあるコンテンツタイプ、配布通路、使用制御情報、監査条件、およびユーザとユーザグループという完全な範囲をサポートすることを可能にする。好適な実施形態におけるVDEオブジェクト作成は、原子エレメント(atomic element)が少なくとも部分的にモジュール制御プロセスを表すVDEテンプレートを採用する。ユーザは、VDE作成ソフトウェア（好適な実施形態においてはGUIプログラミングプロセス）およびVDEテンプレートを採用して、VDEオブジェクト300を作成し得る。VDEオブジェクト300の作成は、例えば、オブジェクトを分割し、「メタデータ」（例えば、著者の名前、作成日など）をオ

ブジェクト内に入れ、オブジェクトに関連する権利及び／又はオブジェクトコンテンツを例えばパブリッシャ及び／又はコンテンツクリエータに割り当てることにより行われる。オブジェクトクリエータは、このプロセスを行うとき、通常必要なデータを要求するコンテンツ仕様手続きを行う。コンテンツ仕様プロセスは、満足されると、例えば、データをテンプレートに挿入してコンテンツをカプセル化することにより進行し得る。さらに、好適な実施形態において、オブジェクトはまたその存在をローカルVDEノード電子機器600の安全なサブシステムに自動的に登録し得る。そして、テンプレート命令と原子メソッド(atomic method)とのインタラクションの結果、１以上のメソッド、予算及び／又はその他のものを含

み得る１以上の制御ストラクチャピースと共に、少なくとも１つの許可記録808が作成され得る。登録プロセスは、予算がオブジェクト用に作成されることを必要とし得る。オブジェクト作成プロセスが初期の配布を特定する場合、管理オブジェクトはまた、１以上の許可記録808、他の制御ストラクチャ、メソッド、及び／又はロードモジュールをも含み得る。

許可記録808は、オブジェクトとユーザとの間の様々な制御関係を特定し得る。例えば、VDE100は、単一のアクセス（例えば、ユーザと権利ユーザとの間の１対１の関係）とグループアクセス（いずれの数の人間もグループとして承認され得る）との両方をサポートする。単一の許可記録808は、単一およびグループアクセスの両方を規定する。VDE100は、複数のユーザが単一の制御予算を予算として共有することを可能にするプロセスである「共有」を提供し得る。追加の制御ストラクチャという概念は、配布、再配布、および監査を含み、最後のものは、計量および予算情報の減少及び／又は移送をサポートする。これらのプロセスの全ては、通常１以上のVDEの安全なサブシステムにより安全に制御される。

テンプレートおよびクラス

VDEテンプレート、クラス、およびフレキシブルな制御ストラクチャは、映画、オーディオレコーディングおよびライブパフォーマンス、雑誌、電話ベースの小売り、カタログ、コンピュータソフトウェア、情報データベース、マルチメデ

ィア、商用通信、広告、市場調査、インフォマーシャル、ゲーム、数的に制御されたマシン用のCAD/CAMサービスなどを作成、改変、販売、配布、再配布、消費、および使用する組織および個人のためのフレームワークをサポートする。これらのクラスを取り囲むコンテキストが変化または進化すると、本発明の好適な実施形態によって提供されるテンプレートが、より広い使用またはより集中したアクティビティのための、これらの変化に適合するように改変され得る。

VDE100の著作は、3つのインプット、すなわち、テンプレート、ユーザインプット、およびオブジェクトコンテンツを作成プロセスに提供し得る。テンプレートは、ユーザ命令および提供されたコンテンツとインタラクトしてVDEオブジェクトを作成するプロセス内において、VDEオブジェクトを作成（及び／又は改変）することができるオブジェクト制御ソフトウェア用の1セットの制御命令及び／又はデータとして作用する。テンプレートは通常、オブジェクト作成及び／又は制御ストラクチャと特に関連している。クラスは、部署の社員、特定のセキュリティクリアランスレベルなど、又は個人及び／又はVDEノードの特別のケースのためのリストなどの、組織内の「自然な」グループを含み得るユーザグループを表す。

例えば、テンプレートは、特定のストラクチャ及び／又はコンポーネントアセンブリを規定するテキストファイルとして表され得る。ストラクチャ及び／又はコンポーネントアセンブリを有するテンプレートは、VDEオブジェクト著作またはオブジェクト制御アプリケーションとして役立ち得る。作成テンプレートは、多くのサブテンプレートから構成され得、上記サブテンプレートは、最低のレベルにおいて、オブジェクト仕様の記述の「原子レベル」(atomic level)を表す。テンプレートは、コンテンツオブジェクトの様々な局面を記述する1以上のモデルと、オブジェクトがどのように作成されるべきかとを表し得る。オブジェクトがどのように作成されるべきかということは、許可記録808及び／又は関連する予算などを作成、変更、及び／又は破棄するために用いられる安全な原子メソッドを採用することを含む。

テンプレート、クラス（グループアクセス下でオブジェクトを採用するユーザ

グループを含む）、およびオブジェクト「独立」許可記録（複数のオブジェクトに関連し得る許可）と別々のVDEプロセスとしての予算および監査をサポートするストラクチャとを含むフレキシブルな制御ストラクチャは、特定の産業及び／又はビジネス及び／又はアプリケーションというコンテキストにおいて本発明により提供され著作に固有の、フレキシブルで構成調整可能な能力に焦点を当てることを補助する。VDEは、広範囲のパワフルな産業において現在採用されている配布シナリオを（部分的にはアプリケーションまたは産業に特異なテンプレートを用いることにより）合理化し且つ含む。従って、現存する産業及び／又はアプリケーション及び／又はビジネスが、コンテンツタイプ、配布方法、価格決定機構、コンテンツ及び／又は関連する管理アクティビティとユーザとのインタラクション、予算などに関連する馴染みの概念を操作することを可能にするために、

動作及び／又はストラクチャのフレームワークを提供することが重要である。

VDEテンプレート、クラス、および制御ストラクチャは、元来フレキシブルおよび構成調整可能に、情報配布および安全な格納条件の範囲を反映し、新しい産業が出現したときにそれに対する効率的な適用を可能にし、現存する産業及び／又はビジネスの進化及び／又は変化を反映し、さらにある許可並びに／又は予算およびオブジェクトタイプに関連し得る１以上のユーザグループをサポートする。VDEテンプレート、クラス、および基本的制御ストラクチャのフレキシビリティは、オブジェクト制御に対して複合的な条件付きプロセスインパクトを有する、VDEの統合および制御メソッドを使用することにより高められる。本発明は、一体的に採用され且つVDE管理オブジェクトとVDEセキュリティ配置およびプロセスと共に採用された場合、ほとんどの商用配布の実施形態に合わせて構成され得るコンテンツ制御および監査アーキテクチャを真に達成する。従って本発明は、予め決められたアプリケーションモデルに適合するように強制することなく、コンテンツプロバイダの条件および好みを完全にサポートする。本発明は、コンテンツプロバイダが配布チャネルを介してコンテンツの権利、制御情報、および流れ（および監査情報の返却）を規定することを可能にする。

オブジェクトコンテンツの改変（追加、隠匿、改変、除去、及び／又は拡張）

オブジェクトに新しいコンテンツを追加することは、本発明により提供される著作の重要な局面である。プロバイダは、１以上のユーザが、プロバイダが提供するコンテンツを追加、隠匿、改変、除去、及び／又は拡張することを許可したいと望むことがあり得る。このようにして、他のユーザは、現存するコンテンツに価値を追加すること、新しし目的のために変更すること、維持すること、及び／又は他の変更を加えることを行い得る。空の及び／又は新規に作成されたオブジェクトにコンテンツを追加する能力もまた重要である。

プロバイダは、コンテンツおよび付随する制御情報を提供するとき、上記コンテンツに対する追加、改変、隠匿、及び／又は消去を可能にする及び／又は制限する制御情報を追加することを選択し得る。この制御情報は、以下のことに関し得る。

●追加、隠匿、改変、及び／又は消去され得るコンテンツの性質及び／又はロケーション、

●改変、隠匿、消去、及び／又は追加され得る、コンテンツの部分、

●追加、隠匿、及び／又は改変されたコンテンツの制御チェーン中及び／又ローカルな位置における、次のVDEコンテナコンテンツ使用に対して必要とされる安全な制御情報、

●プロバイダが特定する告知及び／又はコンテンツ部分は、追加、隠匿、消去及び／又は改変されたコンテンツ、並びに／又は上記追加、隠匿、改変、及び／又は消去が起こったという事実を伴わなければならないという条件、

●コンテンツから除去、隠匿、及び／又は消去され得るコンテンツに関する制限及び／又は条件であって、コンテンツの追加、隠匿、改変、及び／又は消去の量及び／又は程度を含む、制限及び／又は条件の安全な管理、

●改変、隠匿、追加、及び／又は消去が起こったということ、及び／又は上記起こったことの性質をプロバイダに知らせるということ、そして、

●プロバイダコンテンツを改変、追加、隠匿、及び／又は消去することに関する他の制御情報。

プロバイダは、他のユーザが制御された方法で現存するコンテンツに価値を加

える及び／又は現存するコンテンツを維持する機会を確立するために、この制御情報を用い得る。例えば、ソフトウェア開発ツールのプロバイダは、自分達自身が提供したオブジェクトにコメント及び／又は類似のもの及び／又はコメントツールを追加することを可能にし得る。映画のプロバイダは、そのマテリアルにコメント及び／又はプロモーションマテリアルが追加されることを可能にし得る。マシーンツールの所有者にCAD/CAM仕様を提供するプロバイダは、他のユーザが、仕様に関連する命令を含むオブジェクトを改変して、ユーザの装置に用いるために上記命令を改良及び／又は翻訳することを可能にし得る。データベースの所有者は、データベースのフレキシビリティ及び／又は維持を許可するために、他のユーザが、提供されたデータベースオブジェクトに記録を追加するか及び／又はデータベースオブジェクトから記録を除去することを可能にし得る。

制御情報を導入する別の利点は、ユーザが新しい目的のためにコンテンツを変更することをプロバイダが可能にする機会である。プロバイダは、他のユーザが新しいセッティングにコンテンツを提供することを可能にする。

この制御情報をコンテンツに添付するために、プロバイダは、コンテンツの追加、隠匿、改変及び／又は消去を支配するオブジェクト用のメソッドを提供され得、また許可されれば、上記メソッドを設計および実行し得る。このような１以上のメソッドの設計および実行は、PPE650と組み合わされたVDEソフトウェアツールを用いて行われ得る。プロバイダは、その後、オブジェクトにメソッドを添付するか、及び／又はメソッドを別途提供し得る。許可記録808は、他の制御情報と組み合わされた制御情報に関連する条件を含み得る。または、別の許可記録808が用いられ得る。

コンテンツを追加または改変することの重要な一局面は、暗号化／復号化鍵及び／又は新しい又は変更されたコンテンツを安全化するための他の関連する局面の選択である。プロバイダは、これらのプロセスに関連するメソッド中で、暗号化／復号化鍵並びに／又は新しい及び／又は変更されたコンテンツを安全化するための他の関連する局面を作成及び／又は選択するために用いられるべき技術を特定し得る。例えば、プロバイダは、ひとまとまりの鍵、新しい鍵を生成する技

術、鍵を生成するロードモジュールに対するリファレンス、コンテンツを安全化するプロトコル、及び／又は他の類似の情報を含み得る。

別の重要な影響は、新しい鍵が作成及び／又は使用された場合、その新しい鍵の管理である。プロバイダは、このような鍵、およびいずれの鍵が用いられなければならないかというリファレンスがプロバイダに伝送されることを必要とし得る。または、プロバイダは、鍵及び／又は安全化戦略をプロバイダの知識及び／又は制御の範囲外にしておくことを許可し得る。プロバイダはまた、いくつかの鍵は伝送されなければならないが他の鍵はプロバイダの知識及び／又は制御の範囲外にしておくという中間的な立場を選択し得る。

鍵の管理に関連する別の局面は、コンテンツの追加、隠匿、改変、及び／又は消去から生じるオブジェクトに関連する許可の管理である。プロバイダは、VDEの制御情報ユーザのチェーンが、VDE管理コンテンツにアクセスすること及び／又はVDE管理コンテンツを操作することを許可することに関するVDE規則および制御情報、並びに／又は得られたオブジェクトに関連する規則および制御情報の一部または全部を得ることを許可することもあり得るし、しないこともあり得る。例えば、プロバイダは、第１のユーザがオブジェクト内の新しいコンテンツに対するアクセスを制御することを許可して、それによりコンテンツのその部分を用いたいと望む他のいずれのユーザもが第１のユーザから許可を受け取ることを必要とすることを可能にし得る。これにより、プロバイダの裁量によって、ユーザがオブジェクトにアクセスすることの許可をプロバイダから得る必要をなくすことがあり得るし、なくさないこともあり得る。

追加、改変、隠匿、及び／又は消去に関連する鍵は、独立した許可記録または記録808に格納され得る。上記許可記録808は、プロバイダに配送され得、現存する許可記録と混合される可能性がある。または、新しいコンテンツプロバイダの制御下において単独のままにされる可能性もある。初期許可記録808の作成及びコンテンツ、並びに許可記録に関するいずれの制御情報もが、プロバイダによるアクティビティに関連するメソッドにより収集される。上記許可記録の次の改変及び／又は使用は、プロバイダのメソッド、ユーザの行為、またはその両方を含

み得る。許可記録808を改変する及び／又は使用するユーザの能力は、少なくとも部分的に、プロバイダの許可記録に関連する上位の制御情報に依存する。

配布制御情報

広範囲でフレキシブルな商用取引環境を可能にするためには、プロバイダは、制御チェーン内での次のパーティの可能性を不当に制限することなく、配布プロセスに対する確実な制御情報を確立する能力を有するべきである。本発明により提供される配布制御情報は、フレキシブルな積極的制御を可能にする。いずれのプロバイダも、上位の制御情報によって必要とされる以外は、いずれかの特定の制御を含むことも、いずれかの特定の戦略を用いることも必要とされない。むしろ、本発明は、プロバイダが、包括的な制御コンポーネント（例えば、VDEアプリケーション内に含まれる及び／又はVDEアプリケーションと直接コンパチブルである、プロバイダの特定の市場に適したコンポーネントのサブセットとして提供され得る）から選択して、与えられた取り扱い／制御チェーンに適したストラクチャを確立することを可能にする。プロバイダはまた、プロバイダの制御情報を他のユーザが改変することを可能にして制限する制御情報に対する制御情報を確立し得る。

本発明により提供された管理システムは、管理「イベント」を生成する。これらの「イベント」は、システムまたはユーザのいずれかにより開始され、VDE内で保護されている可能性があるプロセスに対応するアクティビティに対応する。これらのプロセスは、許可記録をコピーする、予算をコピーする、監査追跡記録を読む、メソッドをコピーする、予算を更新する、許可記録を更新する、メソッドを更新する、管理ファイルをバックアップする、管理ファイルを修復するなどのアクティビティを含む。いずれかのVDE記録の部分に対する情報の、読み出し、書き込み、改変、更新、処理、及び／又は消去は、管理イベントである。管理イベントは、１以上の記録の１以上の部分に対する１以上の上記アクティビティを行うプロセスを表し得る。

VDE電子機器600が管理イベントに遭遇すると、そのイベントは、典型的には、VDE PPE650と共に処理される。多くの場合、コンテンツへのアクセス及び／又は

コンテンツの使用に一般に関連するイベントの場合のように、管理イベントは、コンテンツプロバイダ（例えば、コンテンツクリエータ、配布者、及び／又はクライアント管理者を含む）により、オブジェクト、オブジェクトのグループ及び／又はクラスに対して特定された制御の一局面として特定される。

例えば、ユーザが、あるオブジェクトを、デスクトップコンピュータからノートブックコンピュータに使用する許可を配布してほしいという要求を開始した場合、生成される管理イベントの１つは、オブジェクトに対応する許可記録のコピーを作成することであり得る。この管理イベントがROS602により検出されると、このタイプのイベント用のEVENTメソッドが存在し得る。EVENTメソッドが存在する場合、EVENTメソッドに関連する計量、課金、および予算もまたあり得る。計量、課金、および予算作成は、プロバイダが許可記録808をコピーすることを可能にし且つ制限することを許可し得る。

例えば、制御プログラムを処理している間に、計量、課金、予算及び／又は監査記録が生成及び／又は更新され得る。上記監査記録は、管理イベントと上記イベントの処理を取り囲む環境に関する情報を記録し得る。例えば、監査記録は、イベントを開始したユーザ及び／又はシステムアクティビティに対するリファレンス、上記イベントの処理の成功または失敗、日付及び／又は時間、並びに／又は関連する情報を含み得る。

デスクトップコンピュータとノートブックコンピュータとの両方を有するユーザの上記の例を参照すると、許可記録のプロバイダは、上記許可記録をコピーする計量器が処理される毎に監査記録を必要とすることがあり得る。監査記録は、プロバイダに、フレキシブルで構成調整可能な制御及び／又は記録環境のオプションを提供する。

ある環境においては、プロバイダが、制御コンポーネントのいずれの局面が、改変、更新、及び／又は消去され得るかを制限することが望ましいことがあり得る。「原子エレメント規定」は、イベント（および従って制御プロセスが残っている場合はその残り）の適用性を、制御コンポーネントのうちのいくつかの「原子エレメント」に制限するために用いられ得る。例えば、許可記録808が図26に

示すフィールド上の「原子エレメント」に分解される場合、イベント処理チェーンは、原子エレメント規定内でこのフィールドのみを特定することにより、例えば、期限切れの日付／時間に関する情報の、ある回数の改変に制限され得る。別の実施例において、許可記録808は、制御セットに基づいて原子エレメントに分解され得る。本実施例において、イベントチェーンは、ある制御セットに作用するイベントに制限され得る。

ある環境においては、プロバイダが、管理プロセスがどのように行われるかを制御することが望ましいことがあり得る。プロバイダは、安全なデータベース610内に格納された配布記録内に、例えば、与えられたイベントが与えられたメソッド及び／又は記録に関連してどのように処理されるべきかを制御および特定するコンポーネントアセンブリ690と共に用いられる情報を、含むことを選択し得る。例えば、プロバイダが、ユーザが許可記録808のコピーを取ることを許可したいと望む場合、プロバイダは内部で許可記録を変更したいと望んでいることがあり得る。例えば、上記のデスクトップコンピュータとノートブックコンピュータとを有するユーザにおいて、プロバイダは、ユーザが、デスクトップコンピュータ内に存在する情報に基づいてノートブックコンピュータを動作させるために必要な情報のコピーを取ることは許可するが、上記情報の更なるコピーがノートブックVDEノードによりなされることは許可しないということがあり得る。本実施例において、上記の配布制御ストラクチャは、デスクトップコンピュータに存在し続けるが、ノートブックコンピュータに送られた動作用の情報は、ノートブックコンピュータからの配布を行うために必要な配布制御ストラクチャを欠く。同様に、配布制御ストラクチャが、あるコンテンツプロバイダにより、配布者であるコンテンツプロバイダに提供され得る。上記配布者において、制御ストラクチャは、許可記録の関連コピーと共にVDEコンテンツコンテナオブジェクトからのコピーがある回数取られることは可能にする。しかし、配布者が作成したコピーを受け取ったエンドユーザが他のVDEノードに配布するために更なるコピーを行うことを許可しないように、許可記録が（例えば、コンテンツプロバイダの仕様ごとに）変更される。

上記の実施例は、１つの可能性のある場合の１つの特定のイベント（コピーすること）に焦点を当てたが、本発明によって考えられるいずれの制御関係の下においても、記録及び／又はメソッドに対する読み出し、書き込み、改変、更新、処理、及び／又は消去のために、同様のプロセスが用いられ得る。他の例は、予算のコピー、計量器のコピー、予算の更新、計量器の更新、監査追跡の圧縮などを含む。

カスタムメソッドの作成

本発明の好適な実施形態において、メソッドは「意のままに」作成され得るか、又は他のメソッドの名前を付けられ得る。これらの２つのモードは、VDE配布プロセスのより高い構成調整可能性、フレキシビリティ、および積極的制御に寄与する。一般に、メソッドを作成することは、メソッドのデータ部分のための必要なアトリビュートまたはパラメータを特定すること、およびその後メソッドを「タイプする」ことを含む。タイピングプロセスは、典型的には、メソッドのいずれかのデータ部分を処理するために１以上のロードモジュールを選択することを含む。メソッド自体に加えて、メソッド作成のプロセスはまた、許可記録に含めるべきおよび許可記録の改変物であるメソッドオプションサブ記録、および配布された記録内の注釈(notation)を生じ得る。メソッドの実行に必要な、いずれかの「標準」ロードモジュールに加えて、追加のロードモジュールおよびこれらのロードモジュールと共に用いられるデータが、許可されるならば特定され得る。これらのイベント処理ストラクチャ制御は、メソッドの配布を制御する。

例えば、セキュリティ予算の場合を考える。典型的な予算の１つの形態は、ユーザを月ごとに10メガバイトの復号化されたデータに制限することであり得る。ユーザは、関連するVDEコンテンツコンテナオブジェクトを使用する権利をノートブックに移動(move)させたいと望み得る。予算クリエータは、ノートブックを同一の量、オリジナルの量の半分、オブジェクトに割り当てられた、移動回数に基づいた量などに制限し得る。予算と関連する配布メソッド（または内部イベント処理ストラクチャ）は、予算クリエータが、含まれる方法論およびパラメータに関して決定を行うことを許可する。言うまでもなく、メソッドの再配布または

正式な配布の際には、互いに異なる配布メソッドが必要となり得る。これらの選択を統合したものが、メソッドに関する許可記録内に格納される。

予算記録の移動のために用いられるプロセスステップの一例は、以下のようなものであり得る。

１）移動する予算をチェックする（例えば、許可された移動の回数を決定するために行われる）。

２）新しい記録に静止フィールドをコピーする（例えば、負担として）。

３）古い記録（オリジナルの予算）内でDecrカウンタをデクリメントする。

４）古い記録内でEncumbranceカウンタをインクリメントする。

５）配布記録を書き込む。

６）新しい記録に配布イベントIDを書き込む。

７）移動計量器をインクリメントする。

８）移動予算をデクリメントする。

９）新しい記録内でDecrカウンタをインクリメントする。

予算の作成

好適な実施形態において、予算を作成するために、ユーザは、グラフィカルユーザインターフェース予算配布アプリケーション（例えば、VDEテンプレートアプリケーション）を操作する。ユーザは、予算のタイプ、満期サイクル、監査などのいずれの必要なフィールドをも書き込む。予算は、ドル、ドイツマルク、円、及び／又は他のいずれの金銭またはコンテンツ測定スキーム及び／又は組織によっても特定され得る。好適な実施形態によるアプリケーションのアウトプットは、通常３つの基本的エレメント、すなわち、作成された各予算記録に対する安全なデータベース６１０の配布部分における注釈、実際の予算記録、および許可記録に含めるメソッドオプション記録を有する。ある環境においては、現存するメソッドオプションが用いられているため、予算プロセスは、メソッドオプションの作成を生じないことがあり得る。通常、このアウトプットの全体が、安全なデータベース６１０及び／又は１以上の管理オブジェクト内において格納により保護されている。

これらは、好適な実施形態における予算配布アプリケーションのための2つの基本的動作モードである。第1の場合において、オペレータは、予算を特定する無制限の権限を有する。このタイプのアクティビティから生じる予算は、オペレータが権利を有する配布プロセスのいずれの局面をも制御するために自由に用いられ得る。上記権利は、使用のある局面を制限する量などの「セキュリティ」予算での使用を含む。例えば、オペレータが「普通の人」である場合、オペレータは、これらの予算を、パーソナルアカウンティングモデルまたはスケジュールに基づいてオブジェクトを自分自身で利用することを制御するために用い得る。オペレータがVISAで承認された人である場合、得られた予算は、配布システム全体に広い影響を与え得る。核となる考えは、このモードが厳密にオペレータによって制御されるということである。

動作の第2のモードは、「別名」予算を作成するために用いられる。これらの予算は、オペレータのシステム内にすでに存在する予算と連結される。オペレータが予算を扱うとき、別名予算上で負担を引き起こす。これらのタイプの予算が作成されると、アウトプットは、互いに連結された2つのメソッドオプションサブ記録、すなわち、名前予算用のメソッドオプションサブ記録と新しく作成された予算用のメソッドオプションサブ記録とを含む。多くの場合、別名予算は、予算クリエータが、許可記録の適切な必要メソッド記録内でメソッドオプションを改変することを承認される場合、オリジナルの予算の代わりに用いられる。

例えば、会社のユーザ（クライアント管理者）が電子機器600内に会社のVISA予算を有すると仮定する。ユーザは、様々な既存の予算および条件を有する社内ユーザのネットワークに予算を配布したいと望む。ユーザはまた、会社のVISA予算の使用を、ある種のオブジェクトに制限したいと望む。これを行うため、ユーザは、ある会社の予算にVISA予算という別名を付ける。その後ユーザは、会社がユーザに操作を許可する全てのオブジェクトに対する許可記録を（もし承認されていれば）改変して、VISA予算に加えて又はVISA予算の代わりに会社の予算を認識するようにする。次いで、ユーザは、他のユーザに新しい許可記録と予算とを配布する。これらのユーザからの監査データが、その後、会社のVISA予算に対す

る負担に対して削減されて、それにより定期的な課金が行われる。

別の実施例においては、顧客が、家族がVISAカードで電子機器を購入することを制御したいと望み、子供たちが過剰な数のビデオゲームで遊ぶことを防止するが、他方では百科事典の使用は無制限に許可したいと望む。この場合、顧客は、２つの予算を作成し得る。第１の予算は、VISAカードに別名を付けられ、百科事典オブジェクト（個々の百科事典オブジェクト及び／又は百科事典オブジェクトの１以上のクラスとして参照符号をつけられる）のみに用いられ得る。上記百科事典オブジェクトは、明確に改変された許可記録内で別名予算を参照する。第２の予算は、例えば、顧客がビデオゲームオブジェクト（ビデオゲームクラス）に使用するために家族に再配布する時間予算であり得る。この場合、第２の予算は、例えば、１日２時間の使用を許可する「自己補充型」セキュリティ／制御予算である。第１の予算は、上記の例と同一の様式で動作する。第２の予算は、ビデオゲーム用の許可記録に新しく必要となったメソッドとして追加される。時間予算はビデオゲームにアクセスするために必要であるため、第２の予算を必要とする効果的な制御路が導入される。すなわち、家族予算を容認するために改変された許可記録のみが、子供達によってビデオゲームのために用いられ得、１日２時間

に制限される。

権利および予算の共有および配布

移動

好適な実施形態によって提供されるVDEの「移動」という概念は、権利および予算の「友好的共有」というケースをカバーする。「移動」の典型的なケースは、いくつかのマシンを所有し１を越えるマシン上で同一のオブジェクトを用いたいと望むユーザである。例えば、ユーザはデスクトップコンピュータとノートブックコンピュータとを所有している。これらは、ユーザがいずれのマシン上でも読みたいと望む、すなわちユーザが一方のマシンから他方のマシンへ権利を移動したいと望む電子新聞を購読している。

「移動」内の重要な概念は、独立した行為という考えである。権利が移動され

る先の電子機器600は、独立して配布者または情報交換所にコンタクトし得る。例えば、上記のユーザは、長期間の旅行にノートブックを持っていき、デスクトップにローカルに接続することなく情報交換所および配布者にコンタクトしたいと望むことがあり得る。

独立した動作をサポートするために、ユーザは、接続に使用している電子機器600とは独立した配布者または情報交換所で、アカウントを規定する。取引は、エンドユーザと情報交換所または配布者との間で、複数のマシン間で独立してトレース可能であり調停可能である。マシン間での権利、予算、およびビットマップまたは組み合わせ計量器の移動の、基本的な動作もまた、サポートされる。

再配布

再配布は、「移動」の「友好的な共有」と正式な再配布との間のUDE中間グラウンドを形成する。再配布は、クリエータ、情報交換所、または配布者および再配布者間に特別なインタラクションを必要としないという意味で、「匿名配布」と考えられ得る。言うまでもなく、クリエータまたは配布者は、再配布を制限する能力も妨害する能力も有していない。

「移動」概念とは異なり、再配布は、独立した動作を示唆しない。再配布者は

再配布された権利及び／又は予算などを受け取るユーザに対する１接点として寄与する。これらのユーザは、再配布者の情報交換所（または及び／又は配布者）アカウントを知らないし、それに対するアクセスも有していない。再配布者は、配布者及び／又は情報交換所からの制限により特に拒絶されない限り、自分自身が再配布する権利及び／又は予算などの監査役として寄与する。再配布先（再配布された権利及び／又は予算などの受け手）が比較的定量化できないワークロードを情報交換所に課しており、さらに再配布者が自分自身で監査可能なリスクを負っている（再配布される全ての権利及び／又は予算などの責任を負っている）ため、再配布者による、再配布先の権利および予算などの監査は、好適な実施形態ではデフォルトケースと考えられる。

配布

配布は、３つのエンティティを含む。クリエータが通常、配布の源である。クリエータは典型的には、制御ストラクチャ「コンテキスト」を設定し、配布ネットワークに送られる権利を制御し得る。配布者は、オブジェクト（コンテンツ）のエンドユーザとオブジェクト（コンテンツ）のクリエータとの間のリンクを形成するユーザである。配布者は、権利および監査データのための双方向コンジットを提供する。情報交換所は、クレジット及び／又は課金サービスなどの独立した金融サービスを提供し得、配布者及び／又はクリエータとして寄与し得る。許可および予算作成プロセスを介して、これらのパーティは共に、権利の使用及び／又は監査アクティビティのタイプと程度とに対する精密な制御を確立し得る。

負担

「負担」は特別なタイプのVDE予算である。いずれかのタイプの予算配布が起こると、「負担」が生成され得る。負担は、権利行使（例えば、使用に対する支払い）目的のオリジナルの予算と区別できないが、負担の額、および負担の場所を追跡するための送出記録を完成させるために必要な全情報に関して配布記録内で独自の様式で識別される。権利行使目的のためには、負担は、オリジナルの予算と同一であるが、追跡目的のためには、独自の様式で識別可能である。

本発明の好適な実施形態において、負担を追跡して調停するために、非対称な監査の場合であっても、ユーザVDEノードと情報交換所とにより、配布イベントIDが用いられる。すなわち、「新しい」負担予算は、追跡の観点からみると独自的であるが、使用の観点からみると区別できない。

回収不能な負担は、VDE配布プロセスにとって良好な中間制御である。負担が回収されなければならない、適切な「グレースピリオド」が導入され得る。この期間が過ぎると、実際の課金または支払いが起こり得る。しかし、インターバルの期間が切れて課金及び／又は支払いがなされた後でも、負担は残り得、後の調停をサポートし得る。この場合、監査役が、ユーザがクレジットを獲得することを許可するか、又はユーザが、負担のかかった予算を含むVDEノードに接続して金額を内部クレジットとして回収し得る。場合によっては、負担が「グレースピリオド」内に回収されない場合、グレースピリオド違反が繰り返された場合、ま

たは回収されない負担が過剰に多い場合は、失われた監査追跡が再配布の特権を無効にするために十分なほど配布者を懸念させ得る。

負担は様々な配布モードにおいて用いられ得る。予算に別名を付すことと共に用いられた場合、負担は、重要な追加の配布可能性を提供する。予算に別名を付す場合、ユーザは、オブジェクトの制御通路に自分自身を置く。すなわち、別名を付された予算は、それを認識するために改変された許可記録と共にのみ用いられ得る。負担は、そのような制限を有していない。

例えば、ユーザは、子供たちが電子VDEノードのVISA予算を用いることを制限したいと望むことがあり得る。この場合、ユーザは、子供たちの、家族の別名を付した予算用のVISA予算上に負担を生成し、オリジナルのVISA予算の透明な負担である、別の負担を妻用に生成し得る。BigCoは、部署のトップにVISA予算を配布し、別名の付されたBigCo予算をユーザに直接配布する、同様の機構を用い得る。

アカウントナンバおよびユーザID

好適な実施形態において、情報交換所へのアクセスを制御するために、ユーザは情報交換所においてアカウントナンバを割り当てられる。アカウントナンバは

安全なデータベース記録に対して、外部者の観点から独自の「インスタンス」価値を提供する。電子機器600サイトの観点からみると、ユーザ、グループ、またはグループ／ユーザIDは記録の独自のインスタンスを提供する。例えば、VISAの観点からみると、あなたのゴールドカードは、アカウントナンバ123456789に属する。電子機器サイト（例えば企業におけるサーバ）の観点からみると、ゴールドカードはユーザID1023に属し得る。VDEノードを用いている複数のユーザ及び／又はユーザグループを有する組織において、このようなユーザ及び／又はユーザグループも同様に独自のユーザIDを割り当てられる可能性が高い。異なる予算及び／又は他のユーザ権利は、異なるユーザ及び／又はユーザグループに割り当てられ得、そして／又は、VDE制御情報は、このような異なるIDを割り当てられたユーザにより、異なる様式で電子コンテンツ及び／又は機器使用に与えられ得

る。言うまでもなく、情報交換所とローカルサイトとの両方が、両方の情報を有している可能性があるが、「使用されたデータ」対「コメントデータ」は視点に基づいて異なる。

「移動」の好適な実施形態のケースにおいて、権利と共に格納されたアカウントナンバはそのままである。配布の他の形態の好適な実施形態においては、配布先に新しいアカウントナンバが必要とされる。これは、システムにより自動的に生成され得るか、または配布者または再配布者により開発された方法に対応している。配布者は、アカウントナンバ（および関連するアクセスシークレット）を各配布先のローカル名前サービス内に維持している。逆に、配布先の名前サービスは、各配布者のユーザIDに基づいてアカウントナンバを格納し得る。この記録は通常、移動の場合、他の記録と共に移動されるか、他の形態の配布中に生成される。

組織（家族を含む）は、新しいユーザまたはユーザグループ用の制御情報（例えば、予算）を作成するときに、独自のユーザIDを自動的に割り当て得る。

条件記録

VDEコンテンツコンテナオブジェクトに対する１以上の必要な許可記録が受け取られる前に上記オブジェクトに関連する権利を行使するための条件および可能性のあるオプションを確立するために、上記オブジェクトのプライベートヘッダ内に条件記録が存在し得る。この記録は、ユーザが、自分自身が何を有しているか、および接続を行う前に配布者から何を必要とするかを確立することを補助する。特定の権利を行使するための条件または可能性が、上記オブジェクトが公になってから変化した場合、改変された条件記録がコンテナ内にオブジェクト（入手可能であり許可されれば）と共に含まれ得るか、または登録が開始される前に配布者から新しい条件記録が要求され得る。配布者は、自分自身が権利を獲得する及び／又は他のユーザに権利を与える能力を有し得るオブジェクトに対応する、条件記録のコレクション及び／又は記述的情報の「カタログ」をオンライン上に維持するか、及び／又はユーザに配布し得る。

監査の通過

VDEの好適な実施形態において、少なくとも２つのタイプの監査があり得る。予算配布の場合、一般に予算の消費を反映する課金記録が収集および処理される必要がある。許可配布の場合、オブジェクトに関連する使用データもまた頻繁に必要とされる。

オブジェクトに対する制御を発効させるため、クリエータはオブジェクトに関連する基本的制御情報を確立し得る。このことは、許可の形成、様々なセキュリティの配布、管理及び／又は金融面での予算、および許可された再配布のレベルなどにおいて行われる。配布者（および再配布者）はさらに、配布者が受け取った権利、予算など（上位制御情報）の範囲内でこのプロセスを制御し得る。

例えば、オブジェクトクリエータは、追加の必要メソッドが、許可記録に自由に追加され、このアクティビティに対して何らの予算も確立せず、この権利の無制限な再配布を許可し得るということを特定し得る。別の例として、クリエータは、使用権が、配布者によって６人のサブ配布者に移動されることを許可し得る。上記サブ配布者の各々は、10,000部のコピーを配布し得るが、再配布の権利がサブ配布者（再配布者）の顧客に割り当てられることは許可されない。別の例として、クリエータは、使用権が僅か10のVDEノードに１レベルのみの配布（再配布なし）で移動されることを承認し得る。コンテンツプロバイダおよび制御情報の

他のコントリビュータは、許可記録及び／又はコンポーネントアセンブリの使用を介して、他のユーザが送られた許可記録内で代理人として行使することを承認された権利を、制御する能力を有する。上記能力は、他のユーザのこのような権利の１つ、いくつか、または全部を制御する権利が許可されるか制限される（制御情報配布モデルに依存して）限りにおいて存在する。配布者が次のユーザのある種の権利を制御することを制限され他の権利を制御することを許可されるという混合モデルを、VDEを用いて構築することが可能であり、望ましいことがしばしばある。いくつかのVDEモデルにおける権利配布のVDE制御は、部分的に又は全体的に、少なくとも配布チェーンのある１以上の「レベル」については、電子コンテンツ制御情報プロバイダによって制御される。上記電子コンテンツ制御情報

プロバイダは、関連するコンテンツのプロバイダではないか、または上記コンテンツ制御情報により制御されるコンテンツの一部分のみを提供するかである。例えば、あるモデルにおいては、情報交換所はまた、ある価値チェーンの参加者に１以上の権利を提供する権利配布エージェントとして寄与し得る。上記１以上の権利は、情報交換所のクレジットを用いる１以上の権利に「添付」され得る。（上記情報交換所が少なくとも部分的に金融情報交換所である場合、このような制御情報プロバイダは、これに代えてまたはこれに加えて他のユーザの権利を反映し得る。）

コンテンツクリエータまたは他のコンテンツ制御情報プロバイダは、ユーザ（配布者など）の予算を作成し得る。これにより、コンテンツオブジェクト用の無制限な数の許可記録が作成されるが、ユーザが時間内の１以上の予期された時点、及び／又はある期間の後に使用を報告しない（監査レポートを提供しない）場合（及び／又はユーザが使用に対する支払いをしない場合、またはユーザとコンテンツプロバイダとの間の契約の他の局面に違反した場合）は、期限切れ／終了プロセスを介してこの権利及び／又は他の重要な使用権が取り消される。この終了（または一時停止または他の特定された結果）は、例えば、制御情報の１以上の局面を暗号化するために採用された時間エージング暗号化鍵の期限切れにより実施される。この同一の終了（または予算削減、価格上昇、ユーザのスクリーン上でのメッセージ表示、管理者へのメッセージなどの、他の特定された結果）

もまた、ユーザまたはユーザVDEインストレーションが監視されたプロセスを完了しなかった結果であり得る。上記監視されたプロセスとは、使用に対する電子通貨での支払い、重要な格納された情報（例えば、コンテンツ及び／又は機器使用情報、制御情報など）のバックアップを取ることができないこと、適切なパスワードまたは他の識別子などを用いないことを繰り返すこと）を含む。

一般に、ある監査役に報告するために収集された監査情報のコレクションは、期限切れ及び／又は他の終了プロセスにより実施され得る。例えば、ユーザのVDEノードは、(a)外部ソースからあるタスクをもう行わないようにと命令されるか、(b)あるタスクをもう行っていないことを知らせる情報をその制御ストラクチ

ャ内に保持しているか、または(c)あるタスクをもう行うことができないかのいずれかである。あるタスクとは、ユーザ（またはインストレーション）が上記監査情報を上記監査役に報告しなかったこと並びに／又は上記監査情報の安全な受け取り確認及び／又は了承を受け取らなかったことによる、１以上の動作開始オペレーションを含み得る。監査役がユーザから監査情報を受け取ることができなかった場合（または他の起こるべきイベントが適切に起こらなかった場合）、例えば本発明の１つの実施形態のセキュリティコンポーネントとして用いられている１以上の時間エージングの鍵がそのエージングを突然加速（完了）し、それによって上記時間エージングの鍵に関する１以上のプロセスがもはや実行され得ないということになり得る。

承認アクセスタグおよび改変アクセスタグ

ユーザVDEインストレーションが監査情報を、情報交換所などのVDE監査パーティに送ることを可能にするために、VDEは、VDE監査パーティが安全に電子的にユーザVDEインストレーションと通信し且つ、上記監査パーティの権利に応じて、上記インストレーションの安全なサブシステム内に格納されているある種の又は全ての情報に関して上記インストレーションに質問をすることを可能にする。（上記パーティは通常、上記パーティが明確にアクセスを承認されていない、安全に格納された情報にはアクセスすることができない。１つのコンテンツプロバイダは通常、異なるコンテンツプロバイダによって提供されたコンテンツに関連

するコンテンツ使用情報にアクセスすることを承認されない。）監査パーティは、上記サブシステムにより維持されるある種の情報にアクセスする、監査役の権利のセットを表す、安全なシークレット（例えば、シークレットタグ）を明確に示す。上記サブシステムが、上記タグの有効性を検査した場合、監査パーティは、要求して受け取ることを許可された監査情報を受け取り得る。

監査追跡条件の実施には大きなフレキシビリティがある。例えば、クリエータ（又はオブジェクトまたは監査レポートの取り扱いチェーン内の、他のコンテンツプロバイダまたは制御情報プロバイダまたは監査役）は、イベント追跡用の監査役による変更を許可するが、クリエータ以外の誰もがそれらの追跡を読むこと

を許可せず、この権利の再配布を例えば６レベルに制限するということがあり得る。これに代えて、クリエータまたは他の制御パーティは、配布者に例えば100,000の監査記録を処理する権利（及び／又は、例えば与えられたユーザからの12の監査記録を処理する権利）を、その使用を報告する前に、配布者に与え得る。クリエータまたは他の制御パーティは、望めば、監査情報を含む別々の（および異なる、サブセット形態の、重複した、または同一の情報を含む）監査「バケット」を許可（及び／又は要求）し得る。上記監査情報のある部分は、配布者によって処理されるべきものであり、上記監査情報の他の部分は、クリエータ及び／又は他の監査役（各々が同一の、重複した、サブセット形態の、または異なる監査情報を受け取る）に戻されるべきものである。同様に、例えばオブジェクトクリエータによって許可される限り、配布者（または他のコンテンツ及び／又は制御情報プロバイダ）は、監査情報が、例えば約50,000の監査記録が処理された後（または他のいずれかの数の監査記録、及び／又はある時間が経った後に、及び／又は予め決められたある日付に）、再配布者によって、元に返却されることを必要とし得る。好適な実施形態において、監査規則は、他の制御ストラクチャ同様、上記規則を特定する権利がより「上位」のオブジェクト及び／又は制御情報を配布する（監査するなど）参加者により制限されていない限り、取り扱いの配布チェーンのいずれかの段階で特定され得る。

異なる監査役に予定されている監査情報は、異なる１以上の暗号化鍵により暗号化され得る。上記暗号化鍵は、各監査役のVDEノードにより安全に提供されて

ユーザの許可記録に含めるために、例えばオブジェクト登録中に必要なステップとして通信される。これは、監査役が承認された監査情報のみにアクセスし得ることをさらに保証するために追加の（パスワード及び／又は他の識別情報および他のVDEセキュリティ特徴を越えた）セキュリティを提供する。一実施形態において、監査情報の暗号化された（及び／又は暗号化されていない）「バケット」（例えば、管理オブジェクトという形態にある）は、異なる監査役に向けられ得る。上記異なる監査役は、情報交換所及び／又は他のコンテンツプロバイダ及び／又は他の監査情報ユーザ（例えば、市場アナリスト及び／又はリストプロバイ

ダを含む）を含む。情報は、VDE監査制御ストラクチャおよびパラメータにより特定されるように、例えば、単一の取り扱いユーザのチェーンを介して、情報交換所から再配布者、さらに配布者からパブリッシャ／オブジェクトクリエータまで、うまく送られ得る。これに代えて、暗号化された（または通常あまり好適ではないが暗号化されていない）監査パケットは、ユーザから複数の監査役に直接分散されることが必要とされ得る。上記監査役の一部は、他の監査役に監査パケットを「パスする」責任を有する。別の実施形態において、監査情報は、例えば、情報交換所に送られ得る。その後、情報交換所は、上記情報（及び／又はいくらかの処理された結果）の全て及び／又は適切なサブセットを１以上の他のパーティに再配布し得る。上記再配布は、上記情報交換所によって作成されたVDEの安全なオブジェクトを用いて行われる。

監査役（監査情報の受け手）の重要な機能は、監査情報が受け取られ及び／又は「認識された」ことを認めた上で、管理イベントをユーザVDEノードに戻すことである。好適な実施形態において、監査情報の受け取り及び／又は容認に続いて、２つのプロセスが行われ得る。第１のイベントは、監査レポートを準備したVDEノードの監査データを消去させるか、または１以上のサマリーバリューに圧縮または追加する。第２のイベントまたはイベントセットは、上記VDEノードの関係するセキュリティ（例えば終了及び／又は他の結果）の制御情報に、監査の受け取りを「告知」し、満期日を改変し、鍵更新及び／又はその他のことを提供する。ほとんどの場合、これらのイベントは、監査追跡が受け取られた後すぐにサイトに送られる。場合によっては、この伝送は、例えば、まず監査追跡及び／又はユーザによる監査役又は他のパーティへの支払いの処理を可能にするために遅延され得る。

好適な実施形態において、コンテンツオブジェクト用の監査イベントと別々に配布されたメソッド／コンポーネントアセンブリとは類似であるが、必ずしも同一ではない。例えば、予算のための鍵更新は、オブジェクトコンテンツの復号化よりもむしろ課金追跡の暗号化を制御し得る。予算のための課金追跡は全ての点で、メソッドイベント追跡である。一実施形態において、この追跡は、情報交換

所による調停を可能にするために、負担の配布記録に対する十分なリファレンスを含み得る。これは、例えば、グレースピリオドが過ぎて、期限切れの負担がクリエータに「返却」された場合に、予算のクリエータが、未回収の負担が最終的に自動クレジットを生み出すことを許可すれば、起こる。

取り扱い通路を介した監査記録の配送は、部分的に、逆（情報の返却）監査メソッドにより保証され得る。多くのVDEメソッドは、少なくとも2つのピース、すなわち、ユーザのVDEノードにおいて監査情報を生成するプロセスを管理する部分と、その後監査データに作用する部分とを有する。複数の監査役に割り当てられた監査情報を取り扱う一実施例において、単一のコンテナオブジェクトが、情報交換所（又は他の監査役）に受け取られる。このコンテナは、(a)情報交換所自体が使用する、ある種の暗号化された監査情報、および(b)1以上の他の監査役パーティに向けられた、ある種の他の暗号化された監査情報を含み得る。2つの情報セットは、同一の、重複した、および部分的に異なる、又は完全に異なる情報コンテンツを有し得る。これに代えて、情報交換所のVDEノードは、提供された監査情報の一部または全部で仕事をすることができることがあり得る。監査情報は、部分的に又は全体的に、情報交換所で更に処理された、ある種の要約及び／又は分析された形態にあり得る。そして／又は、上記監査情報は、他の情報と組み合わされて、引き出された情報セットまたは少なくともその一部を形成し、そして1以上の少なくとも部分的に安全なVDEオブジェクトに挿入されて上記1以上の（更なる）監査パーティと通信されることがあり得る。監査情報コンテナが上記情報交換所のVDEノードにおいて上記逆（返却）監査メソッドにより安全に処理されると、情報交換所のVDEノードは、監査情報を他の監査役に安全に運搬し且つ上記情報交換所によって使用されることが特定された安全な監査情報を別途処理する、1以上のVDE管理オブジェクトを作成し得る。VDE参加者間の安全な監査処理およびクレジット情報配布は、通常、安全なVDE「ブラックボックス」内で起こる。すなわち、監査情報は、安全なVDE PPE650内で処理が安全に行われ、監査情報は、VDE参加者のVDEの安全なサブシステム間で、VDEの安全な通信技術（例えば、公的な鍵暗号化および認証）を用いて安全に通信される。

このタイプの逆監査メソッドは、例えば監査情報のローカルな処理及び／又は監査情報の１以上の監査パーティへの安全な送付を含む、返却された監査情報の取り扱いを特定し得る。必要とされ得るように、及び許可記録仕様及び／又は改変プロセス中に、１以上の他の監査パーティ及び／又はコンテンツプロバイダ及び／又は制御情報プロバイダにより設定されていることがあり得る基準に応じて、監査情報が１以上の監査パーティに送られない場合、例えば、監査パーティ、例えばコンテンツプロバイダが必要とされる監査情報がうまく移送されたことを知らせることに失敗すると、その結果、パーティのVDEノードを介した送信の多少の性能がなくなり得る（例えば、上記監査又はパーティに関連するオブジェクトに関する、ある１以上のVDE管理ビジネス機能を更に行う能力がなくなり得る）。この好適な実施形態においては、オブジェクトが監査役に受け取られると、オブジェクトは自動的に登録され、許可記録のコンテンツが監査役のVDEノードの安全な管理データベースに入れられる。

監査レポートオブジェクトの作成および使用を管理する（そしてオブジェクトの使用の他の局面もまた管理し得る）１以上の許可記録が、監査情報レポート交換（又は、ユーザと監査役または監査エージェントとの間の他の電子インタラクション）中に、ユーザのシステムにより受け取られ得る。受け取られた許可記録の各々は、次の監査レポートオブジェクトを支配し得る。監査情報の報告後、次の監査レポートサイクル用の監査レポート作成および監査情報移送を管理する能力をリフレッシュするために、新しい許可記録がユーザのVDEノードで必要とされ得る。上記の実施例において、監査レポートの目的で監査役が１以上の許可記録をユーザに供給することを可能にすることは、監査役（情報交換所など）がある種の特定された許可記録自体を「上流の」監査役（例えば、コンテンツ及び／又は他のコンテンツ制御情報プロバイダなど）から受け取っていることを必要とし得る。これらの上流の許可記録により提供された情報は、監査役のVDE（例えば情報交換所）インストレーションにおいて、１以上の許可記録に一体化され得る。上記インストレーションは、監査情報レポート交換中に、ユーザに向けられた許可記録を含む管理オブジェクトを生成する許可記録作成サイクルを管理する

。上流の監査役が必要とされる監査情報を受け取れない場合及び／又は処理できない場合、この上流の監査役は、情報交換所（本実施例の場合）に、与えられた１以上のオブジェクト（またはオブジェクトクラス）用の次の許可記録作成／監査サイクルを配布者がサポートすることを可能にする、必要な許可記録情報を提供することができないことがあり得る。その結果、情報交換所のVDEノードは、ユーザ用の次のサイクルの許可を記録生成すること及び／又は何らかの他の重要なプロセスを行うことができないことがあり得る。このVDE監査レポート制御プロセスは、全体的に、意図された監査情報の受け手と送り手との両方におけるイベント駆動型VDEアクティビティを含み、安全なPPE650と安全なVDE通信技術との両方を採用する、電子プロセス管理である。

好適な実施形態において、ユーザが新しいオブジェクトをユーザ自身のVDEノード、及び／又はこれに代えて遠隔の情報交換所及び／又は配布者のVDEノードに登録する毎に、１以上の許可記録が少なくとも部分的に上記オブジェクトの使用を支配するために提供される。許可記録は、安全なUDE登録プロセス中にダイナミックに（VDEインストレーションの安全なサブシステムを用いて）提供され得るか、及び／又は初期登録後に提供されて、それに続く何らかの時点で、例えば、１以上の別々の安全なVDE通信を介して、受け取られることがあり得る。上記安全な通信は、例えば、上記情報を含む又は運搬する物理的配置を含む。１以上の許可記録をユーザに提供することに関連する少なくとも１つのプロセスは、計量イベントを引き起こし得る。計量イベントの結果、監査情報が、ユーザのVDEノード、情報交換所、及び／又は配布者の許可記録提供プロセスを反映して作成される。この計量プロセスは、１以上の許可記録が作成されたことを記録するのみでないことがあり得る。計量プロセスはまた、VDEノードの名前、ユーザネーム、関連するオブジェクト識別情報、時間、日付、及び／又は他の識別情報を

も記録し得る。この情報の一部または全部は、情報交換所または配布者により、例えば、監査コンテンツクリエータ及び／又は他のコンテンツプロバイダに安全に報告された監査情報の一部となり得る。この情報は、受け取る監査役のサイトにおいて、上記情報交換所または配布者により上記監査役に送られたユーザの監

査情報に対して、安全なVDEアプリケーションソフトウェアにより調停され得る。ある種の１以上のVDEオブジェクトを管理し及び／又はVDEオブジェクト監査レポートの作成を管理するために、あるユーザ（及び／又はVDEノード）のために作成された、計量された１以上の許可記録（または記録セット）の各々について、監査役が、少なくとも部分的に暗号化された監査レポートに組み込まれた、対応する監査情報を受け取ることが望ましいことがあり得る。許可記録の作成の計量、安全な暗号化された監査情報の報告プロセス、登録及び／又は受け取られた監査レポート詳細を含む監査報告許可の作成を反映する計量情報の、安全なVDEサブシステムによる調停、および１以上の安全なVDEインストレーション期限切れ及び／又は他の終了及び／又は他の結果プロセスは、組み合わせられると、信頼できる、効率的な商用環境としての、VDEの安全な監査報告プロセスの完全性を高める。

安全な文書管理例

安全な文書管理環境を提供するために、VDE100が使用され得る。以下は、いかにしてこれが達成され得るかのいくつかの例である。

１つの実施例において、法律事務所が文書を管理するためにVDE100を用いることを望んでいるとする。この実施例において、訴訟チームの一部である法律事務所は、以下の様式でVDEを用い得る。

１．秘匿なクライアント記録へのアクセス及び／又は上記クライアント記録の他の使用を安全に制御する様式。

２．法律事務所で作成された文書および覚書へのアクセス、上記文書および覚書の配布、及び／又は上記文書および覚書に関する他の権利を安全に制御する様式。

３．事件に関連する調査資料へのアクセスおよび上記調査資料の他の使用を安全に制御する様式。

４．事件に関連する記録、文書およびメモへのアクセス、および上記記録、文書およびメモの、配布を含む、他の使用を安全に制御する様式。

５．コメントおよび検討用に配布された法的文書（brief）を訴訟チームの他の

法律事務所がどのように使用し得るか及び変更し得るかを安全に制御する様式。

６．クライアントへの請求の管理を補助する様式。

法律事務所はまた、裁判所に法的文書を電子的に提出するために（裁判所もVDEを使用可能であると考えて）VDEを用い得る。この使用は、提出者のID（例えば、ディジタル署名）の監査の検証および上記提出手続に関連する他の情報を含む。

本実施例において、法律事務所は、VDEコンテンツコンテナ内に、クライアントの、VDEにインストールされた安全なサブシステムから文書を受け取る。これに代えて又はこれに加えて、法律事務所は、スキャンされて電子形態にされ得る紙媒体の文書を受け取ってもよいし、及び／又はVDEコンテナ内にまだ入れられていない電子文書を受け取ってもよい。電子形態の文書は、特定のクライアント及び／又は事件に関連するVDEコンテナ（オブジェクト）として格納される。VDEコンテナ機構は、コンテナ内でファイルおよび他の情報を系統立てるための階層命令スキームをサポートする。この機構は、コンテナ内で文書の電子コピーを系統立てるために用いられ得る。VDEコンテナは、コンテナに関連する１以上のパーミッション制御（PERC）情報セットに記述された特定のアクセス制御情報および権利に関連する。本実施例において、法律事務所の所員のうち、VDEインスタンス、適切なPERC、および所望の文書を含むVDEオブジェクトを有する所員のみが文書を用い得る。これに代えて又はこれに加えて、法律事務所の所員は、法律事務所のネットワークサーバにインストールされているVDEインスタンスを用い得る。この場合、所員は、（サーバVDEインストレーションを用いるためには）適切なPERCにより識別され且つVDEオブジェクトを含む文書へのアクセスを有していなければならない。電子文書に対する基本的なアクセス制御は、１以上のユーザVDEにインストールされた安全なサブシステムを用いることにより可能になる。

VDEは、いくつかの方法で基本的使用制御を提供するために用いられ得る。第１に、単一のオブジェクト内に複数のコンテナを「埋め込む」ことを許可する。埋め込まれたオブジェクトは、コンテナ内の制御ストラクチャを「ネスティン

グ」することを許可する。VDEはまた、使用制御情報を、任意の細分性レベル（従来のオペレーティングシステムにより提供されるファイルベースのレベルではなく）にまで拡張し、VDE制御されたプロセスとして記述され得る情報に関連するいずれのアクションに関するフレキシブルな制御情報をも提供する。例えば、簡単な制御情報は、文書の１以上の部分を見ることに関連し得、追加の制御情報は、これらの同一の文書の同一の及び／又は１以上の異なる部分を編集、印刷およびコピーすることに関連し得る。

本実施例において、「クライアント」コンテナは、クライアントにより提供された全ての文書を含む（他のコンテナ内に受け取られた文書は、VDE抽出埋め込み能力を用いて安全に抽出されてVDEクライアントコンテナに埋め込まれ得る）。本実施例中の各文書は、ペアレントであるクライアントVDEコンテナ内にオブジェクトとして格納される。「クライアント」コンテナはまた、内部に埋め込まれた他のいくつかのオブジェクトを有する。そのうちの１つは各弁護士がクライアントに関するメモを格納するためであり、１つ（またはそれ以上）は、調査結果および関連情報用であり、そして少なくとも１つは、法律事務所によって作成されたレター、ワークペーパーおよび法的文書の副本用である。クライアントコンテナはまた、課金、時間、決算および支払いの電子記録を含む、クライアントに関する他の情報を含み得る。ペアレントVDEコンテンツコンテナ内にVDEオブジェクトを埋め込むことは、類似の制御情報を共有する異なる情報を安全に類別及び／又は格納するための便利な方法を提供する。クライアントにより提供された全ての文書は、例えば、使用および非開示に関する同一の制御ストラクチャに供され得る。弁護士のメモは、制御情報に供され、例えばその使用は、メモを作成した弁護士と作成した弁護士がアクセス権を明確に許可した弁護士とに限られ得る。埋め込まれたコンテナはまた、異なる情報の集まりを制御するための便利な機構を提供する。例えば、調査オブジェクトは、オブジェクトによってなされる調査の結果を含むVDE「スマートオブジェクト」という（またはそれから由来した）形態で格納され得る。VDEにより与えられたLEXISサイトから検索された、事件の一局面に関する調査結果は、１つのスマートオブジェクトとしてカプセル化され得る。事件の別の（または同一の）局面に関連する別のセッションの結果は

、異

なるオブジェクトとしてカプセル化され得る。本実施例において、スマートオブジェクトは、完全に離散し且つ別々に配送された制御情報が、プロバイダ（コンテンツの所有者など）の権利を行使するために望まれ及び／又は必要とされるクライアントコンテナに組み込まれ得るということを示すことを補助するために用いられる。

制御ストラクチャは、いずれの所望の細分性及び／又は論理的文書コンテンツの、文書、ページ、段落、トピックの面で関連する資料などによるグルーピングをも管理するために用いられ得る。本実施例において、以下のように仮定する。クライアントにより提供された文書はページレベルで制御され、弁護士のメモは弁護士別に文書レベルで制御され、裁判所の記録および法的文書は、文書レベルで制御され、調査情報は、調査が行われたときにコンテンツのプロバイダが特定する何らかののレベルで制御される。上記の様々なコンテンツ内に位置するある種の非常に秘匿性の高い情報は、表示およびリードパートナーである弁護士による追加コメントのためのみのサブジェクトとして識別され、与えられたコンテンツのクリエータ及び／又は埋め込み者のみが他の方法による使用（印刷、抽出、配布など）を行う権利を有する。

概して、本実施例におけるコンテナのコンテンツは、権利の配布に関して制御される。この制御情報は、内部で作成された全ての文書に関しては文書レベルで、クライアントレベルの文書に関してはページレベルで、そして調査文書に関してはコンテンツプロバイダにより特定されたレベルで関連づけられる。

VDE制御情報は、参加者の要望に応じて、複雑なストラクチャまたは単純なストラクチャのいずれかで構成され得る。ある場合には、VDEクリエータが、使用したいと望む（そして規則および制御情報の仕様を管理するVDEアプリケーションにより、直接、またはアプリケーションとコンパチブルであることが証明されたVDEコンポーネントアセンブリを介してサポートされている）一連の制御ストラクチャ定義を適用する。

本実施例において、法律事務所は、新規クライアントに対して、事件を引き受

けた時点で、標準VDEクライアントコンテンツコンテナをセットアップする。法律事務所のVDE管理者は、新規クライアント用のVDEグループを設立し、その事件に関して作業をすることを承認された法律事務所の弁護士のVDE IDを加え、且つ適切であれば、１以上のユーザテンプレートアプリケーションを提供する。これらのテンプレートは、例えば、（上位制御情報により許可されれば）追加の及び／または代わりの制御機能のユーザによる選択、制御パラメータデータのエントリ、及び／またはユーザが特定する管理タスクの実行のための１以上のユーザインターフェースおよび関連するストラクチャを提供する。管理者は、コンテナを作成するために予め規定された作成テンプレートに沿って作成ツールを用いる。この作成テンプレートは、上記の文書の使用形態（配布制御情報を含む）を特定する。次いで、クライアントからの各電子文書（レター、覚書、Ｅメール、スプレッドシートなど）が別途埋め込まれたオブジェクトとしてコンテナに追加される。新しいオブジェクトの各々は、与えられたタイプの新しいオブジェクトの各々にとって必要とされるコンテナに対して特定されたデフォルト制御ストラクチャを満足する作成テンプレートを用いて作成される。

各弁護士は、事件に関する作業を行う際に、クライアントのVDEコンテナ内に格納されたオブジェクトにメモをエンターし得る。これらのメモは、すでに法律事務所で用いられている、VDE認識ワードプロセッサを用いて取られ得る。本実施例において、VDEリディレクタは、ワードプロセッサファイルの要求を、１以上のVDE PPEで動作するVDE制御プロセスを用いて、VDEコンテナおよびそのオブジェクトに安全にマッピングする。弁護士のメモのオブジェクトは、文書タイプがコンテンツから自動的に決定され得ない場合は、弁護士の援助を得て文書タイプ用のデフォルト作成テンプレートを用いて作成される。これにより、VDEが、予め決められたレベル、例えば文書、ページ、段落レベルで、メモを自動的に検出および保護することが可能になる。

調査は、VDEを用いて自動的に管理され得る。スマートオブジェクトは、安全なサーチを行い、必要であれば、インフォーメーションハイウェイ上のVDEイネーブルド情報リソースから情報に対して支払いを行い且つ情報を検索するために

用いられ得る。

このようなリソースの例は、LEXIS、Westlaw、および他の法律関係のデータベースを含み得る。情報は、一旦検索されれば、VDEコンテンツクライアントコンテナ内に安全に埋め込まれ得る。スマートオブジェクトがまだ、未放出の情報を含んでいる場合、スマートオブジェクト全体がクライアントのVDEコンテナ内に埋め込まれ得る。このことは、未放出の情報を二重のVDE制御条件下、すなわち、スマートオブジェクトからの情報（支払い及び／又は監査に関する必要条件）を放出することに関する必要条件下、および特定のタイプのクライアント情報へのアクセスまたは上記クライアントの情報の他の使用に関連する必要条件下に置く。

法的文書および他のファイリングは、弁護士のメモに類似の様式で制御され得る。ファイリングは、法律事務所の標準のワードプロセッサを用いて、編集され得る。この編集は、使用制御ストラクチャが誰が文書（またはより高度な例においては、文書のある部分）を検討し、変更し、及び／又は追加を行い得るかを制御する状態で行われる。VDEはまた、時間／日付のスタンプを押すことおよびファイルされた文書の有効性検査のための信頼できるソースを提供することにより法的文書の電子ファイリングをサポートし得る。

クライアントおよび弁護士が電子メールまたは他の手段で秘匿情報を交換したいと望むとき、VDEは、情報が、特権により守秘が許可され(privileged)且つ適切に制御され、不適に放出される及び／又は用いられることがないことを保証する上で重要な役割を果たし得る。VDEコンテンツコンテナオブジェクト内に格納されたマテリアル（コンテンツ）は通常暗号化される。このようにラップされた状態において、VDEオブジェクトは、承認されないアクセス及び／又は他の使用が行われるおそれなく、受け手に配布される。オブジェクトを受け取った１人以上の承認されたユーザが、そのオブジェクトを開いて見る及び／又はそのコンテンツを操作及び／又は改変し得る唯一のパーティであり、VDEの安全な監査は、全てのこのようなユーザコンテンツのアクティビティの記録を保証する。VDEはまた、必要であれば、例えば、ユーザの使用監査情報を管理者が検討した後に、

クライアントと弁護士との間の、特権により守秘が許可された情報を用いる権利を取り消すことを許可する。

大組織の例

より一般的な例において、広い地域に亘って数千～数十万人の従業員および多数の事務所をかかえる組織（例えば、企業または政府の官庁）が、その組織（または協会）に属する情報の配布を制御することを望んでいるとする。この情報は、公式文書、電子メールメッセージ、テキストファイル、マルチメディアファイルなどの形態をとり得、これらを総合して「ドキュメント」と呼ぶ。

このようなドキュメントは、人間（「ユーザ」と呼ぶ）及び／又はユーザの代わりに動作するコンピュータにより取り扱われ得る。ドキュメントは、格納および伝送用の電子形態と手動取り扱い用の書類形態との両方で存在し得る。

これらのドキュメントは、全体的に組織から発される場合もあるし、全体もしくは一部が組織外から受け取られた情報から作成される場合もある。組織内の承認された人は、ドキュメントの全体または一部を、組織外のエンティティに放出することを選択し得る。このようなエンティティのなかには、ドキュメント制御のためにVDE100を採用し得るものも、し得ないものもある。

ドキュメント制御ポリシー

組織は全体として、ドキュメントへのアクセス制御及び／又はドキュメントの他の使用制御に関する十分に定義されたポリシーを有し得る。このポリシーは、情報の流れの「格子モデル」に基づき得る。情報の流れにおいて、ドキュメントは１以上の階層「分類」セキュリティアトリビュート9903と０以上の非階層「コンパートメント」セキュリティアトリビュートとを有するとして特徴づけられ、これら全てが共にセンシティビティセキュリティアトリビュートを構成する。

分類アトリビュートは、ドキュメントのセンシティビティの全体的なレベルを、順序がつけられたセットのエレメントとして指定し得る。例えば、政府関係においては「アンクラシファイド」「コンフィデンシャル」「シークレット」「トップシークレット」というセットが適切であり得、企業関係においては、「パブリック」「インターナル」「コンフィデンシャル」「レジスタードコンフィデン

シャル」というセットが適切であり得る。

コンパートメントアトリビュートは、部署のサブディビジョン（例えば、「調査」「開発」「マーケティング」）などの、組織内の１以上の特定のアクティビティ、または組織内の特定のプロジェクトの、ドキュメントとの関係を指定し得る。

電子機器600を用いる各人は、承認されたユーザにより、これらのドキュメントまたはあるドキュメントタイプの１以上の部分を指定するための、１セットの許可されたセンシティビティアトリビュートを割り当てられる。上記文書又は部分は、その人の電子機器によって１以上の方法で処理され得る。ドキュメントのセンシティビティアトリビュートは、アクセス可能となるためには、許可されたセンシティビティ値のユーザセットに属していなければならない。

さらに、組織は、ユーザがある規定された責任を有する特定のドキュメントに関しては、ユーザが制御することを許可することを望み得る。例えば、ユーザ（作成ユーザ(originating user)）があるドキュメントに対して「作成者により制御された」（「ORCON」）制約をつけたいと望むことがあり得る。上記制約は、例えば、ドキュメントが、そのユーザが指定する特定の他のユーザのみによって（しかもある明確に承認された方法によってのみ）伝送および使用され得るようにつけられる。ドキュメントの作成の後、特に誰かが承認された受け手のオリジナルリスト以外の受け手に作成ユーザからドキュメントを伝送することを要求した場合に、「配布リスト」が改変され得るならば、このような制約はフレキシブルであり得る。発信ユーザは、特定のユーザ、規定されたユーザグループ、規定された地域、特定の組織的役割内で行動することを承認されたユーザ、またはこのようなアトリビュートのいずれか若しくは全てのみに対する配布を許可したいと望むことがあり得る。

本実施例において、組織はまた、ドキュメントへのアクセスは上記のように制限されるがドキュメント内の情報の一部または全体が受け手による更なる制約なしに抽出および再配布され得るというような、より弱い配布制約をユーザが規定することを許可したいと望むことがあり得る。

組織及び／又は発信ユーザは、ドキュメントがどのような使用のために、またはいずれの地域に配布されているかを知りたいことがあり得る。組織は、ある種の保護アトリビュートを有するドキュメントがどこに配布されているかを、例えば、サイトコンフィギュレーション記録及び／又はネームサービス記録に格納された地理的情報に基づいて、知りたいと望むことがあり得る。

ユーザは、配布されたドキュメントに対する「リターンレシート」を要求したいと望むことがあり得、またはドキュメントが受け手によりどのように取り扱われているか（例えば見られているのか、印刷されているのか、編集されているのか、及び／又は格納されているのか）を、例えば、そのドキュメントに関連するPERC内の１以上の監査必要条件（または監査必要条件を有することが知られているメソッド）を特定することにより、知りたいと望むことがあり得る。

ユーザ環境

上述したような組織（または協会）において、ユーザはドキュメントを処理および管理するための様々な電子機器600を利用し得る。これは、ネットワークに接続された又はされていないパーソナルコンピュータ、パワフルシングルユーザワークステーション、およびサーバまたはメインフレームコンピュータを含み得る。本実施例に記載する制御情報に対するサポートを提供するために、VDE保護ドキュメントの使用および管理に参加している各電子機器が、SPE503及び／又はHPE655をサポートする、VDEの安全なサブシステムにより向上され得る。

安全な動作に関する脅威が比較的低いいくつかの組織においては、HPE655で十分であり得る。他の組織（例えば政府の安全保障機関）においては、VDE保護ドキュメントが処理される全ての状況においてSPE503を採用する必要があり得る。向上した環境および技術の選択は、異なる組織においては異なる。異なる必要条件を満たすために異なるタイプのPPE650が組織内で用いられている場合であっても、それらは互いにコンパチブルであり得、同一のタイプ（または同一のタイプのサブセット）のドキュメント上で動作し得る。

ユーザは、VDE保護ドキュメントを扱うためにVDEと協同して動作するようにカスタマイズされたアプリケーションプログラムを用い得る。上記アプリケーショ

ンプログラムの例は、VDE認識ドキュメントビューワ、VDE認識電子メールシステム、および類似のアプリケーションを含み得る。これらのプログラムは、VDE保護ドキュメントを入手可能としながらも、そのコンテンツがコピーされ、格納され、見られ、改変され、及び／又は伝送され、及び／又はさらに特定の電子機器の外部に配布される程度を制限するために、ユーザの電子機器600のPPE650コンポーネントと通信し得る。

ユーザは、VDE保護ドキュメントを処理するために、市販の既製（「COTS」）オペレーティングシステムおよびアプリケーションプログラムを採用したいと望み得る。COTSアプリケーションプログラムおよびオペレーティングシステムの使用を許可する１つのアプローチは、再配布に関する制約なしにドキュメントのみのために、上記の使用を可能にすることである。標準VDEオペレーティングシステムリディレクタは、ユーザが、ファイルへのアクセスと等価な様式でVDE保護ドキュメントにアクセスすることを可能にする。しかし、このようなアプローチの場合、使用を計量及び／又は監査する制御のチェーンが、保護されたオブジェクトがCOTSアプリケーションに入手可能になったときに、ある程度「壊れ」得る。いずれの放出された情報の更なるトラッキングを容易にするためにも、VDEの指紋刻印（ウォーターマーキング）技術が用いられ得る。

保護されたドキュメントの印刷を保護するために、例えばサーバベースの復号化エンジン、「指紋刻印」用特別フォントなどの、様々な技術が用いられ得る。

COTSソフトウェアをサポートするための別のアプローチは、COTSオペレーティングシステムおよびアプリケーションプログラムが走り得るが、VDEの制御下以外では、いかなる情報も永久的に格納されることもなく伝送されることもない、１以上の「仮想マシン」環境を生成するために、ユーザの電子機器上で走るVDEソフトウェアを用いることである。このような環境は、VDEが全てのVDE保護情報を管理することを許可するが、限定された環境内で情報を処理するためにCOTSアプリケーションを無制限に用いることを許可し得る。このような環境のコンテンツ全体が、VDE100により、環境に読み込まれたいずれのVDE保護ドキュメントに対する拡張としても扱われ得る。環境外部への情報の伝送は、オリジナルドキュ

メントと同一の規則で支配される。

「粗い」制御能力

上記のように、組織は、ドキュメント全体のセキュリティ、配布、完全な状態の維持、および制御を管理するために、VDE強化制御能力を用い得る。これらの能力のいくつかの例は、以下のものを含み得る。

１）２以上の電子機器600を接続する通信チャネルは、１セットの許可されたセンシティビティアトリビュートを割り当てられ得る。センシティビティアトリビュートがこのセットに属するドキュメントのみが、チャネルを介して伝送されることを許可される。このことは、Trusted Computer System Evaluation Criteria(TCSEC)のDevice Labels必要条件をサポートするために用いられ得る。

２）電子機器600に接続された又は組み込まれた書き込み可能記憶装置（例えば、固定ディスク、ディスケット、テープドライブ、光ディスク）は、１セットの許可されたセンシティビティアトリビュートを割り当てられ得る。センシティビティアトリビュートがこのセットに属するドキュメントのみが、装置に格納されることを許可される。このことは、TCSEC Device Labels必要条件をサポートするために用いられ得る。

３）ドキュメントは、ドキュメントを「取り扱う」ことを許可されたユーザを表す、ドキュメントに関連したユーザのリストを有し得る。このユーザリストは、例えば、ドキュメントを見ることができるユーザのみを表し得る。他のユーザは、たとえドキュメントコンテナを受け取っても、コンテンツを操作し得ない。このことは、標準ORCON取り扱い警告をサポートするために用いられ得る。

４）ドキュメントは、その作成者を指定してドキュメントのコンテンツが見られ得る前に作成者による明確な許可が下されることを必要とするアトリビュートを有し得る。この許可に対する要求は、ドキュメントがユーザによってアクセスされたとき、または例えばあるユーザが他のユーザにドキュメントを配布したときになされ得る。許可が下りない場合、ドキュメントは操作も使用もされ得ない。

５）ドキュメントは、ドキュメントの各使用がドキュメントの作成者に報告さ

れることを必要とするアトリビュートを有し得る。このことは、ドキュメントの配布を計測(gauge)するために作成者により用いられ得る。その使用が使用時に制御パーティに知られていることを保証するために、必要であれば、ドキュメントのいずれの使用もが許可される前に、レポートがうまくなされていることが必要とされ得る。これに代えて、例えばレポートは据え置き（「バッチ」）様式でなされ得る。

６）ドキュメントは、ドキュメントの各使用が中央ドキュメントトラッキング情報交換所に報告されることを必要とするアトリビュートを有し得る。このことは、特定のドキュメントをトラッキングするため、特定のアトリビュート（例えばセンシティビティ）を有するドキュメントをトラッキングするため、いずれかの特定のユーザ及び／又はユーザグループにより用いられたドキュメントを識別するためなどに、組織により用いられ得る。必要であれば、例えば、ドキュメントのいずれかの使用が許可される前に、レポートがうまく行われていることが必要であり得る。

７）VDE保護ドキュメントは、ドキュメントの各使用が作成者への「リターンレシート」を生成することを必要とするアトリビュートを有し得る。ドキュメントを用いる人は、リターンレシートを生成するために、例えば、ドキュメントがなぜ興味を引くのかを示すことにより、またはドキュメントコンテンツのリターンレシートに関する知識を（読んだ後）示すことにより、特定の質問に答えることを必要とされ得る。このことは、ドキュメントが自動化されたソフトウェア機構によってではなく人によって取り扱われたことを保証するために用いられ得る。

８）VDE保護ドキュメントのコンテンツは、独自の様式で、コンテンツを放出したユーザまで識別可能（トレース可能）であるように、VDEを認識しないアプリケーションプログラムにとって、入手可能とされ得る。従って、ドキュメントの放出された形態がさらに配布されても、その源は決定され得る。このことは、コンテンツ放出用VDE「指紋刻印」を採用することにより行われ得る。同様に、印刷されたVDE保護ドキュメントは、コピーがなされていても、類似のVDE指紋刻

印された独自の様式で、はじめにドキュメントを印刷した人が決定され得るように、マークされ得る。

９）VDE保護ドキュメントの使用は、ドキュメントコンテンツへのアクセスまたは上記コンテンツの他の使用を（サイズ、アクセス時間などに基づいて）制限する予算の制御下において許可され得る。このことは、固定期間中に個人にアクセス可能なVDEドキュメントの数を制限することにより、大規模な開示を防止することを補助し得る。例えば、このような制御の１つは、ユーザが、何らかの特定の分類レベルのドキュメントに関して、１日最大100ページを見るが１日10ページのみを印刷することを許可し、印刷を平日の９時から５時までのみ許可することである。さらなる例として、ユーザは、例えば（通常またはいずれかの合理的な状況下における）１以上のタイプの超過データベース使用が起こったことを識別するために、VDE保護ドキュメントの使用の、ある量の論理的に関連する比較的「連続した」及び／又は何らかの他のパターン（フィールド内のある識別子を共有する記録量に基づいてデータベースの記録の使用を制限するなど）に制限され得る。その結果、VDEコンテンツのプロバイダは、VDEコンテンツの使用を、容認可能な使用特性に制限し得、例えば情報データベースリソースの、ユーザによる不適切な使用の試みを（例えばVDE管理者または組織監督者用の例外レポート(exception report)を生成することにより）防止及び／又は識別し得る。

これらの制御能力は、センシティブなドキュメントをトラッキングし管理するためのフレキシブルでインタラクティブな環境を提供するために、VDEがどのように用いられ得るかのいくつかの例を示す。このような環境は、人から人へのドキュメントの流れを直接、物理的位置、組織などごとにトレースし得る。さらに、「R&D部外のどの人がR&D制御されたドキュメントを受け取ったか」というような特定の質問に答えることを許可する。制御情報は、VDE保護ドキュメントの各コピーと共に伝送され、中央レジストリが更新されること及び／又は作成者がドキュメントの使用を知らされることを保証し得るため、トラッキングは即刻行われ得、且つ正確であり得る。

このことは、紙のドキュメントをトラッキングする従来の手段と矛盾する。従

来の手段によると、典型的には手動で収集され且つ取り扱われたレシートの紙ベースのシステムが用いられる。ドキュメントは個々にコピーナンバが付され署名されるが、一旦配布されれば能動的に制御されない。従来の紙ベースのシステムにおいては、ドキュメントの実際の位置を決定することは実際不可能である。どのような制御が示され得るかは、全てのパーティが厳密に取り扱い規則（最高の状態であっても不便である）を守った場合のみ決定可能である。

上記状況は、通常のコンピュータおよびネットワークシステムのコンテキスト内でドキュメントを処理するために、たいして都合よくはない。上記システムはユーザアイデンティティに基づくアクセス制御情報を強化し得、且つファイルへのアクセスをトラッキングする監査機構を提供し得るが、これらはコンテンツの

流れのトラッキングも制御も許可しない低レベルの機構である。このようなシステムにおいては、ドキュメントコンテンツが自由にコピーされ且つ操作され得るため、ドキュメントコンテンツがどこに行ったか、またどこから来たかを決定することは不可能である。さらに、通常のコンピュータオペレーティングシステム内の制御機構は抽象的な低レベルで動作するが、オペレーティングシステムが制御するエンティティは、必ずしもユーザによって操作されるエンティティと同じではない。このことは特に、監査追跡を、興味を引かないアクティビティを記述する大量の情報により混乱させる。

「細かい」制御能力

ドキュメント全体を制御および管理することに加えて、ユーザは、ドキュメントの個々の改変を制御および管理するために、カスタマイズされたVDE認識アプリケーションソフトウェアを採用し得る。これらの能力の例は以下を含む。

１）VDEコンテンツユーザは、提案された代わりのワーディングを示すために、VDEドキュメントに更なる情報を追加することを許可され得る。この提案された変更は、（オリジナルテキストに加えて）ドキュメントの全ての他のユーザに可視であるが、（例えば）ドキュメントの所有者によってのみ実際のテキストに組み込むことができる。

２）VDEユーザグループは、個々の変更がそれを行った特定のユーザにまで明

確にトレース可能であるような様式で、ドキュメントの１以上の部分を改変することを許可され得る。ドキュメントのある部分を改変する権利、および異なるユーザに対する異なる権利セットの拡張は、組織または安全な環境が、同一のコンテンツのユーザに異なる権利を与える異なる許可を提供することを可能にする。

３）ユーザグループは、VDEドキュメントを、個々の寄稿物(contribution)から作り上げることにより量を増加する様式で作成し得る。これらの寄稿物は、単一の制御されたドキュメント内でまとめられ得るが、各々の寄稿物は、例えば埋め込まれたコンテナオブジェクトとしてVDEコンテンツコンテナ内に組み込まれることにより個々に識別される。

４）VDE制御および管理能力は、例えばドキュメントの各セクションが何回見られたかを記録する、個々のドキュメントエリアに関連するアクティビティをトラッキングするために用いられ得る。

実施例：VDE保護コンテンツ格納場所

「ディジタルハイウェイ」が出現すると、ネットワーク、特にインターネットなどの公的なネットワークでのコンテンツの配布に関する議論が増す。コンテンツは、以下を含むいくつかの方法で公衆ネットワークを介して入手可能にされ得る。

● 要求による又は事前の購入（物を購入するために電子基金またはクレジットの債務を表すトークンを送ること）に応答してユーザへコンテンツを「メールする」こと。

● 組織自体のコンテンツ格納場所からダウンロード可能なコンテンツをサポートすること。このような格納場所は、例えば、通常１以上のデータベースに系統立てられる大量の製品（ソフトウェアプログラムなど）及び／又は大量の情報リソースを含む。

● 他のパーティが顧客への再配布のために製品を預け得る公的な格納場所をサポートすること（通常、要求に応答して顧客への配布のために電子コピーを作成することによって行われる）。

VDEノードの１つの可能性のあるは、１以上の「格納場所」の使用を含む。例

えば、格納場所はVDE参加者がそこからVDEコンテンツコンテナを検索し得るロケーションとして作用し得る。この場合、VDEユーザは、１人以上のVDEユーザがVDEコンテンツコンテナを含むオブジェクト格納場所にアクセスすることを可能にする「サーバ」システムへのアクセスを獲得するためにネットワークを利用し得る。

何人かのVDE参加者は、コンテンツ及び／又はVDEコンテンツコンテナオブジェクトを作成または提供し、その後他の参加者が知られた及び／又は（検索用に）効果的に系統立てられたロケーションにアクセスし得るように格納場所にコンテンツ及び／又はコンテンツオブジェクトを格納し得る。例えば、VDE格納場所（VDE格納場所の一部、複数のVDE格納場所、及び／又はそのような格納場所へのコンテンツのプロバイダ）は、ネットワークユーザのリストにＥメールを送信することにより、あるタイプのVDE保護コンテンツが入手可能であることを宣伝し得る。ネットワークユーザが電子機器内に安全なVDEサブシステムを有している場合は、ネットワークユーザは、そのような格納場所に直接または１以上のスマートエージェントを介してアクセスすることを選択し得る。そして、ネットワークユーザは、例えばアプリケーションプログラムを用いて、格納場所において入手可能なVDE管理コンテンツの提供をブラウズ（及び／又は電気的にサーチ）し、所望のVDEコンテンツコンテナをダウンロードし、そのようなコンテナを利用し得る。格納場所がうまくそのようなコンテンツに興味を持つユーザを引き付けれた場合、VDEコンテンツのプロバイダは、そのような格納場所がそのコンテンツをユーザにとって容易にアクセス可能にするための望ましいロケーションであると決定し得る。CompuServeのような格納場所が暗号化されていない（平文）形態でコンテンツを格納する場合、格納場所は、所望の制御情報を有するVDEコンテンツ内に「送出する」コンテンツを入れることによって、「送出する」コンテンツを「必要に応じて」暗号化し得、VDE参加者へのコンテンツの通信用の、VDEの安全な通信技術を採用し得る。

VDE格納場所はまた、他のVDEサービスをも提供し得る。例えば、格納場所は、格納場所から得られるVDEオブジェクトの使用に関連する料金を支払うために用

いられ得る、格納場所からのクレジットという形態で、金融サービスを提供することを選択し得る。これとは別にまたはこれに加えて、VDE格納場所は、VDEユーザにより報告された使用情報に関して、VDEクリエータまたは他の参加者（例えば、配布者、再配布者、クライアント管理者など）に代わって監査情報交換所サービスを行い得る。このようなサービスは、このような使用情報を分析すること、レポートを作成すること、料金を収集することなどを含み得る。

「フルサービス」のVDE格納場所は、VDE管理コンテンツのプロバイダとユーザとの両者にとって非常に魅力のあるものであり得る。VDE管理コンテンツのプロバイダは、そのコンテンツをユーザによく知られたロケーションに置くこと、クレジットを提供すること、及び／又はユーザのための監査サービスを行いたいと望むことがあり得る。この場合、プロバイダは、コンテンツを「小売り」様式で

入手可能にすること、多くのVDEユーザから監査情報を収集すること、請求書を送付して料金を受け取ることなどに関連する管理上のプロセスを監督するよりも、コンテンツを作成することに集中できる。VDEユーザは、単一のロケーション（またはまとめて配置された複数の格納場所）の便利さが、興味を引くコンテンツを探そうと試みたときに魅力的であることを理解し得る。さらに、フルサービスVDE格納場所は、VDE格納場所から受け取られたVDE管理コンテンツを使用した結果生じる使用情報を報告するため及び／又は例えば更新されたソフトウェア（例えば、VDE認識アプリケーション、ロードモジュール、コンポーネントアセンブリ、非VDE認識アプリケーションなど）を受け取るための単一のロケーションとして作用し得る。VDE格納場所サービスは、VDEユーザのコンテンツに対するニーズを満たすために、ブラウズされ、サーチされ、及び／又はフィルタをかけられ得るコンテンツリソースの統合的アレイを構成するために、放送による及び／又はCD-ROMなどの物理的媒体上でのVDEコンテンツ配送と共に用いられ得る。

公的な格納場所システムは、非営利または営利サービスとして設立されて維持され得る。サービスを提供する組織は、例えば取引ベース及び／又は料金のパーセンテージベースで、及び／又はユーザの負担で、ユーザへのコンテンツごとにサービス料金を課金し得る。格納場所サービスは、コンテンツクリエータ、パブ

リッシャ、配布者、及び／又は付加価値プロバイダにVDE著作ツールを供給し得、上記の人々がコンテンツの使用を管理するガイドラインの一部または全体を規定する規則および制御を適用し、そのようなコンテンツをVDEコンテンツコンテナオブジェクトに入れることができるようになっている。

格納場所は、１つのロケーションに維持されてもよいし、異なるロケーションにあるが単一のリソースを構成し得る様々なサーバ（例えばビデオサーバなど）のような様々な電子機器に配布されてもよい。VDE格納場所の配置は、VDEの安全な通信およびVDEノードの安全なサブシステム（「保護課の処理環境」）を採用し得る。ユーザが望む情報の与えられたひとまとまり又はユニットを含むコンテンツは；様々な物理的ロケーションに散らばっていることがあり得る。例えば、会社の株式終値と株式に関する活動（付け値、安値、高値など）とを表すコンテンツは、ニューヨークのWorld Wide Webサーバに位置し、会社の分析（社史、人事、製品、市場、及び／又は競合相手に関する考察）を表すコンテンツは、ダラスのサーバに位置するというようなことがあり得る。コンテンツは、使用を安全にし監査するために、VDE機構を用いて格納され得る。コンテンツは、このような１以上のサイトで他の形態のセキュリティ（例えば、物理的セキュリティ、パスワード、保護されたオペレーティングシステム、データ暗号化、またはあるコンテンツタイプに適した他の技術）が十分入手可能であれば、クリアな形態に維持され得る。後者の場合、コンテンツは、少なくとも部分的に暗号化され、格納場所から送出されるときにVDEコンテナ内に置かれ、それにより、安全な通信ならびにそれに続くVDEユーザ使用制御および使用結果管理を可能にする。

ユーザは、株式および他の情報を含む、会社に関する情報を要求し得る。この要求は、例えば、まずディレクトリまたはボストンにあるより高度なデータベース配置を介してルートされ得る。このアレンジメントは、ニューヨークとダラスの両方の格納場所へのポインタを含み、両方の格納場所からコンテンツを検索し得る。この情報コンテンツは、例えば、２つのコンテナ（例えば、ダラスからのVDEコンテンツコンテナオブジェクトとニューヨークからのVDEコンテンツコンテナオブジェクト）内のユーザに直接ルートされ得る。これらの２つのコンテナは

、ユーザの電子機器により処理されたとき、単一のVDEコンテナ内に２つのVDEオブジェクトを形成し得る（上記単一のVDEコンテナは、ダラスとニューヨークとからのそれぞれのコンテンツを含む２つのコンテンツオブジェクトを含み得る）。これに代えて、このようなオブジェクトは共に統合されてボストンの単一のVDEコンテナを形成し得、それにより、情報が単一のコンテナでユーザに配送されてユーザサイトでの登録および制御を簡素化する。両方のロケーションからの情報コンテンツは、別々の情報オブジェクトとして格納されてもよいし、単一の統合された情報オブジェクトとしてまとめられてもよい（情報形態またはテンプレートの、あるフィールド及び／又はカテゴリは、１つのリソースで満たされ得、他のフィールド及び／又はカテゴリは、異なるリソースにより提供された情報によって満たされ得る）。配布されたデータベースは、VDE制御のVDEの電子的実施を介した情報の格納、送信、監査及び／又は使用を安全化するために、このような配布された格納場所リソース環境を管理しVDEを用い得る。この場合、VDEは、

—

貫したコンテンツコンテナとコンテンツコンテナサービスとの両方を提供するために用いられ得る。

１つの可能性のある格納場所配置3300の実施例を図78に示す。本実施例において、格納場所3302は、ネットワーク3304に接続され、ネットワーク3304は、著者3306A、3306B、3306Cおよび3306D、パブリッシャ3308、ならびに１人以上のエンドユーザ3310が格納場所3302と通信すること及び互いに通信することを可能にする。第2のネットワーク3312は、パブリッシャ3308、著者3306Eおよび3306F、エディタ3314、ならびに司書3316が互いに通信すること及びローカル格納場所3318と通信することを可能にする。パブリッシャ3308はまた、著者3306Eと直接接続されている。本実施例において、著者3306とパブリッシャ3308とは、エンドユーザ3310が共通のロケーションから広範囲のコンテンツにアクセスすることができる環境にコンテンツを置くために、格納場所3302に接続されている。

本実施例において、格納場所は２つの主要な機能領域、すなわち、コンテンツシステム3302Aと情報交換所システム3302Bとを有する。コンテンツシステム3302

Aは、ユーザ／著者登録システム3320と、コンテンツカタログ3322と、サーチ機構3324と、コンテンツ格納部3326と、コンテンツリファレンス3328と、送出システム3330とを含む。送出システム3330は、制御パッケージャ3322と、コンテナパッケージャ3334と、取引システム3336とを含む。情報交換所システム3302Bは、ユーザ／著者登録システム3338と、テンプレートライブラリ3340と、制御ストラクチャライブラリ3342と、分配システム3344と、承認システム3346と、課金システム3352と、監査システム3360とを含む。承認システム3346は、金融システム3348と、コンテンツシステム3350とを含む。課金システム3352は、ペーパーシステム3354と、クレジットカードシステム3356と、電子基金送金システム(EFT)3358とを含む。監査システム3360は、レシートシステム3362と、レスポンスシステム3364と、取引システム3366と、分析システム3368とを含む。

本実施例において、著者3306Aは、著者3306Aが多くのエンドユーザ3310に広く入手可能にし且つVDEの使用を介して自分の権利を保護しようと意図するコンテンツを電子形態で作成する。著者3306Aは、メッセージを格納場所3302に伝送して、自分のコンテンツを配布するために格納場所に登録したいという要望を示す。

このメッセージに応答して、コンテンツシステム3302Aのユーザ／著者登録システム3320と、情報交換所システム3302Bのユーザ／著者登録システム3338とが、ネットワーク3304を用いて登録情報に対する要求を著者3306Aに伝送する。これらの要求は、オンラインインタラクティブモードにおいてなされてもよいし、著者3306Aにバッチ様式で伝送されてもよい。その後、著者3306Aは、要求された情報を完成させて格納場所3302にバッチ様式で伝送する。または、ある局面はオンラインで（基本的な識別情報として）取り扱われ、他の情報はバッチ様式で交換されてもよい。

コンテンツシステム3302Aに関連する登録情報は、例えば、以下を含む。

● 著者3306Aが、格納場所を用いて格納およびアクセスすることを提案されたコンテンツのタイプ及び／又はカテゴリに関する情報を提供すべきであるという要求。

●アブストラクト及び／又は格納場所によって必要とされた他の識別情報の形態。これは、著者3306Aに、著者3306Aが概してコンテンツ提出と共に他の情報（プロモーションマテリアル、提出されたコンテンツのフォーマットに関する詳細な情報、提出されたコンテンツを使用する可能性のあるユーザがうまくその価値を利用するために満たすべき又は満たさなければならない装置条件など）を含むかどうかを示す機会を与えることに加えてである。

●コンテンツがどこに位置されるか（格納場所内に格納されるのか、著者3306Aのロケーションに格納されるのか、どこか他の場所か又は組み合わされた複数のロケーションに格納されるのか）に関して著者3306Aから情報を得たいという要求。

●いずれの一般的なサーチ特性がコンテンツ提出と関連すべきかということ（例えば、アブストラクトが格納場所のユーザがサーチできるように自動的にインデックスを付されるのかどうか、コンテンツのタイトル、アブストラクト、プロモーションマテリアル、関連する日付、パフォーマー及び／又は著者の名前、またはコンテンツ提出に関連する他の情報が、コンテンツのタイプリストにおいて及び／又はサーチに応答して用いられ得るか、又は用いられるべきであるかなど）。そして／又は、

●格納場所内に格納されている及び／又は格納場所を通過するコンテンツがいかにして送出されるべきかということ（コンテンツ伝送に関するコンテナ基準、暗号化条件、取引条件、他の制御基準など）。

情報交換所のユーザ／著者登録システムにより著者3306Aから要求された情報は、例えば、以下のものを含む。

●制御情報を正確にフォーマットするために、著者3306Aが利用し得るか、又は利用しなければならないVDEテンプレート。上記フォーマットは、例えば、情報交換所システム3302Bの監査システム3360が、著者3306Aにより提出されたコンテンツに関連する使用情報を受け取ること及び／又は処理することを適切に承認されるように行われる。

●提出されたコンテンツに関連して著者3306Aにより作成及び／又は使用され

るVDEコンポーネントアセンブリの一部または全部において、著者3306Aにより使用され得るか又は使用されなければならない（及び/又は参照のため含まれ得る又は含まれなければならない）情報交換所3302Bから入手可能なVDE制御情報。

● 格納場所情報交換所システム3302Bにより提供されるか、これを通過するか、またはこれにより収集されるコンテンツの使用に関連するいずれかの基金の分配が行われるべき様式。

● 提出されたコンテンツ及び/又はコンテンツに関連する金融取り引きを用いることを承認する形態及び/又は基準。

● コンテンツ及び/又はコンテンツに関連する情報（他人によって用いられ得る分析レポートなど）の使用に対する課金の容認可能な形態。

● VDEにおいて生成された監査情報がいかにして受け取られるべきかということ。

● ユーザからの要求に対するレスポンスをいかにして管理すべきかということ。

● 監査情報の受け取りに関連する取り引きがいかにしてフォーマットされ承認されるべきかということ。

● 使用情報に関して、どのような形態の分析がいかにして行われるべきかということ。そして／又は

● VDE制御コンテンツ使用情報からの使用情報及び/又は分析結果が管理されるべき状況というものがあるならば、その状況はどのようなものかということ（誰に配送され得るか又は配送されなければならないかということ、配送の形態、そのような情報の使用に関連するいかなる制御情報などをも含む）。

格納場所3302は、著者3306Aから完成した登録情報を受け取り、この情報を用いて著者3306Aのアカウントプロフィールを作成する。さらに、著作プロセスに関連するソフトウェアが著者3306Aに伝送され得る。このソフトウェアは、例えば、著者3306Aが、適切な制御で、VDEコンテンツコンテナ内にコンテンツを置くことを可能にする。適切な制御とは、このようなコンテナを作成することに関連する決定の多くが、コンテンツシステム及び/又は情報交換所システムとしての

格納場所3302の使用を反映させるように自動的になされるように、行われる（上記決定とは、例えば、コンテンツのロケーション、コンテンツ及び/又はコンテンツに関連する制御を更新するためにコンタクトすべきパーティ、監査情報が伝送され得る及び/又はされなければならないパーティとこのような通信のための通信路、使用中に収集される監査情報の特性、コンテンツの使用に対して容認可能な支払いの形態、監査伝送が必要である頻度、課金の頻度、コンテンツに関連するアブストラクト及び/又は他の識別情報の形態、コンテンツ使用制御情報の少なくとも一部分の性質などである）。

著者3306Aは、自分自身がVDEコンテンツコンテナ内に置きたいと望む制御およびコンテンツを特定するためにVDE著作アプリケーションを利用し、格納場所3302のいかなる必要条件にも応じて、そのようなコンテナを作成する。VDE著作アプリケーションは、例えば、格納場所3302によって提供されるアプリケーションであり得、上記アプリケーションは、格納場所コンテンツ制御条件に忠実であることを保証する助けになり得る。上記制御条件とは、1以上のタイプのコンポーネントアセンブリまたは他のVDE制御ストラクチャ及び/又は必要であるパラメータデータ、別のパーティから受け取ったアプリケーション、並びに/又は全体的にまたは部分的に著者3306Aが作成したアプリケーションを含むことなどである。その後著者3306Aは、ネットワーク3304を用いて、コンテナと、上記コンテンツに関連し得る著者3306Aのアカウントプロフィールからの何らかの偏差とを、格納場所3302に伝送する。格納場所3302は、提出されたコンテンツを受け取り、その後、本実施例においては何らかのアカウントプロフィール条件、偏差及び/又は所望のオプションに応じて、コンテンツがコンテンツ及び/又は格納場所の制御情報条件の範囲内で作成されたか否か、そして従ってコンテンツ格納部内に置かれるべきか又はロケーションポインタなどにより参照されるべきか否かを判定する。提出されたコンテンツをコンテンツ格納部内に置くこと、又はそのようなコンテンツのロケーションを参照することに加えて、格納場所3302はまた、サーチ機構3324、コンテンツリファレンス3328、送出システム3330、並びに/又は情報交換所システム3302Bの、テンプレートおよび制御ストラクチャ、承認、課金

及び/又は支払い、分配、及び/又は使用情報に関連するシステム内の、上記提出されたコンテンツに関連する特性に留意し得る。

著作プロセス中に、著者3306Aは、VDEテンプレートを使用し得る。このようなテンプレートは、VDE著作アプリケーションの一局面として用いられ得る。例えば、このようなテンプレートは、上記のようにコンテナの構築において用いられ得る。これに代えて又はこれに加えて、このようなテンプレートはまた、提出されたコンテンツが格納場所3302に受け取られたときに用いられ得る。このようなテンプレートに対するリファレンスは、提出されたコンテンツのコンテナを構築する一局面として、著者3306Aにより組み込まれ得る。（この意味では、格納場所に配送されたコンテナは、ある意味では、指示されたテンプレートの使用を介して格納場所がコンテナを「完成させる」までは「不完全」であり得る。）このようなリファレンスは、格納場所3302による使用にとって必要とされ得る。（格納場所3302による使用とは、例えば、格納場所のビジネスまたはセキュリティモデルの一局面を満たすために、VDE制御情報を適所に置くことである。格納場所のビジネスまたはセキュリティモデルの一局面とは、格納場所のある種の計量、課金、予算作成、及び/又は他の使用及び/又は分配に関連する制御を提供するために、他のVDE制御ストラクチャとインタラクトするために必要な、コンテンツのエレメントに対応する1以上のマップテーブルなどである。）

例えば、著者3306Aによって提出されたコンテンツが、定期刊行物により構成される場合、著者が格納場所に登録したときに格納場所3302により著者に配送されるテンプレートは、著者がそのような定期刊行物のためのVDEコンテンツコンテナを作成する際に操作される著作アプリケーションの一局面として用いられ得る。これに代えて又はこれに加えて、定期刊行物に使用されるように設計されたテンプレートは、格納場所3302にあり得、このようなテンプレートは上記コンテナに関連する制御ストラクチャを全体的に又は部分的に定義づけるために格納場所により使用され得る。例えば、定期刊行物用の制御ストラクチャを形成することを補助するように設計されたVDEテンプレートは（特に）以下のことを示し得る。

●使用制御は、ユーザが開く刊行物内の各記事を記録するメータメソッドを含むべきである。

●定期刊行物を開くためには、開かれる記事の数にかかわらず、ある一定の一律料金が適用されるべきである。そして／又は

●ユーザが見た全ての広告の記録が維持されるべきである。

コンテンツが、知られた及び／又は識別可能なフォーマットで維持されている場合、このようなテンプレートは、このような記録および課金行為をサポートするために必要とされ得るいずれかのマップテーブルを識別するために著者3306Aが介入することなしに、コンテナの初期構築中に用いられ得る。このようなVDEテンプレートが著者3306Aに入手可能でない場合、著者3306Aは、提出されたコンテナが、あるテンプレートまたはある分類レベルのテンプレートにおいて特定されたVDE制御情報を含むように格納場所によって再構築（例えば、増大）されるべきであるということを示すことを選択し得る。コンテンツのフォーマットが、知られた及び／又は格納場所により識別可能なものである場合、格納場所はこのようなコンテナを自動的に再構築する（または「完成する」）ことができることがあり得る。

格納場所と著者3306Aとの間の潜在的な金融面での関係の１つの要因は、提出されたコンテンツの、エンドユーザ3310による使用に関連し得る。例えば、著者3306Aは、格納場所が、格納場所のサービス（例えば、エンドユーザ3310に対してコンテンツを入手可能にすること、電子クレジットを提供すること、課金アクティビティを行うこと、料金を集めることなど）を維持することと交換に、エンドユーザ3310から発生した全収益の20％を確保することを承認する、格納場所との取り決めをネゴシエートし得る。金融面での関係は、フレキシブルで構成変更可能な方法で制御ストラクチャ内に記録され得る。例えば、上述した金融面での関係は、著者3306Aの金融面での条件と、収益を格納場所と分けて20％を取る必要性とを反映させるために著者3306Aが考案したVDEコンテナ及び／又はインストレーション制御ストラクチャ内で作成され得る。上記の場合、提出されたコンテンツの使用に関連する全ての課金アクティビティが格納場所によって処理され得、

著者3306Aの提出したコンテンツを使用するために必要とされる様々なコンポーネントアセンブリに関連する反復的方法を表す制御ストラクチャが収益の20%を計算するために用いられ得る。これに代えて、格納場所は、価格の上昇を反映させるために、著者3306Aからの制御ストラクチャを独立に且つ安全に追加及び／又は改変し得る。ある場合においては、著者3306Aは、格納場所が使用アクティビティに対して課する実際の価格には直接関与しない（または実際の価格を知らない）こともあり得る。著者3306Aは、収益の量と、VDE制御コンテンツの使用および使用の結果を支配するVDE制御情報内で著者3306Aが特定する、自分自身の目的のために必要である使用分析情報の特性のみに関心があるということがあり得る。

著者と格納場所との関係の別の局面は、VDE制御コンテンツの配送とVDE制御コンテンツ使用監査情報の受け取りとに関連する取り引き記録条件の特性を含み得る。例えば、著者3306Aは、格納場所が格納場所からコンテンツのコピーを受け取った各ユーザの記録を取ることを必要とし得る。著者3306Aはさらに、このようなユーザへのコンテンツの配送の環境（例えば、時間、日付など）に関する情報の集まりを必要とし得る。さらに、格納場所は、このような取り引きを内部で使用する（例えば、システムを最適化するための使用パターンを決定する、詐欺を検出するなど）ために行うことを選択し得る。

このようなVDE制御コンテンツの配送に関する情報を記録することに加えて、著者3306Aは、格納場所がある種のVDEコンテナ関連プロセスを行うことを必要としたか又は要求したということがあり得る。例えば、著者3306Aは、異なる分類レベルのユーザには、異なるアブストラクト及び／又はその他の記述的情報を配送したいと望み得る。さらに、著者3306Aは、例えば、特定のユーザによって提示された使用の特性に応じて、提出されたコンテンツと同一のコンテナで、プロモーションマテリアルを配送したいと望み得る（上記使用の特性とは、例えば、ユーザはこれまで著者3306Aからコンテンツを受け取ったことがあるか否か、ユーザは著者3306Aのマテリアルをよく購読しているか否か、及び／又はある種のVDEコンテンツエンドユーザに配送されるプロモーションマテリアルを混ぜたもの

を決定することを補助するために用いられる、著者3306A及び／又はエンドユーザに関連し得る他のパターンである）。別の実施例においては、著者3306Aは、コンテンツがエンドユーザに伝送される前に、このようなコンテンツに対してVDE指紋刻印が行われることを必要とし得る。

エンドユーザに送出されるコンテンツの形態及び／又は特性に加えて、著者はまた、ある種の暗号化関連プロセスが、コンテンツを配送することの一局面として格納場所によって行われることを必要とし得る。例えば、著者3306Aは、格納場所が、コンテンツのよりよい保護を維持することを補助するために、異なる暗号化鍵を用いて、送出されるコンテンツの各コピーを暗号化することを必要としたということがあり得る。（上記コンテンツのよりよい保護とは、例えば、暗号化鍵が「クラックした」すなわち誤って開示されても、その「ダメージ」は配送可能なあるコンテンツの特定のコピーの一部分に制限され得るということである。）他の実施例においては、暗号化機能は、環境による条件を満たすために（例えば、輸出のための制限に従うために）、完全に異なる暗号化アルゴリズム及び／又は技術を用いる必要性を含み得る。さらに別の実施例においては、暗号化関連プロセスは、コンテンツが配送されるVDEサイトの信頼性レベル及び／又は不正改変不可能性レベルに基づいて、暗号化技術及び／又はアルゴリズムを変更することを含み得る。

コンテンツがVDE格納場所からエンドユーザに送出されるときに集められる取り引き情報に加えて、格納場所は、使用情報、要求、及び／又はエンドユーザ3310からの及び／又はエンドユーザ3310へのレスポンスに関連する取り引き情報を保持することを必要とされ得る。例えば、著者3306Aは、格納場所が、著者3306Aのコンテンツの使用に関する情報（例えば、監査情報のエンドユーザレポート、追加の許可情報に対するエンドユーザからの要求など）の送信及び受信に関連して、エンドユーザ3310が行う接続の一部または全部の記録を取ることを必要とし得る。

格納場所を介してエンドユーザ3310に提供されるVDE管理コンテンツのうちのいくつかは、コンテンツ格納部に格納され得る。他の情報は、他の場所に格納さ

れ、コンテンツリファレンスを介して参照され得る。コンテンツリファレンスが使用されている場合、格納場所は、コンテンツ格納部に格納されているか他の場所（別のサイトなど）に格納されているかにかかわらず、全ての格納場所のコンテンツが、例えば一貫した又は同一のユーザインターフェースのように均一な様式でエンドユーザ3310により選択されるために提示されるように、ユーザインターフェースを管理し得る。エンドユーザが、コンテンツ格納部に格納されていないコンテンツの配送を要求した場合、VDE格納場所は、コンテンツリファレンスに格納されている情報（例えば、コンテンツが位置し得るネットワークアドレス、URL、ファイルシステムリファレンスなど）を用いてコンテンツの実際の格納サイトを探し出し得る。コンテンツが探し出された後、コンテンツはネットワークを介して格納場所まで伝送されてもよいし、又は格納されている場所から要求しているエンドユーザに直接伝送されてもよい。ある状況においては（例えば、コンテナの改変が必要であるとき、暗号化が変更されなければならないとき、金融取り引きが放出前に必要であるときなど）、このようなVDE管理コンテンツ及び／又はVDEコンテンツコンテナをエンドユーザに伝送するために準備するために、格納場所による更なる処理が必要であり得る。

VDE格納場所のエンドユーザ3310にとって入手可能なコンテンツへの管理可能なユーザインターフェースを提供し、エンドユーザ3310に送出されるVDEコンテンツコンテナ内にパッケージされた制御情報の決定において用いられる管理情報を提供するために、本実施例の格納場所は、コンテンツカタログ3322を含む。このカタログは、コンテンツ格納部内のVDEコンテンツに関連する情報、及び／又はコンテンツリファレンス内に反映された格納場所を介して入手可能なコンテンツを記録するために用いられる。コンテンツカタログ3322は、コンテンツのタイトル、アブストラクト、および他の識別情報から構成され得る。更に、カタログはまた、電子契約及び／又は契約VDEテンプレートアプリケーション（オプションの選択可能な制御ストラクチャ及び／又は関連するパラメータデータを提供する1以上の機会）という形態を示し得る。上記契約およびアプリケーションは、例えば以下のことに対するオプション及び／又は必要条件を決定する際に、与え

られたコンテンツ用の格納場所を介してエンドユーザ3310に入手可能である。いずれのタイプの情報がコンテンツの使用中に記録されるか、あるコンテンツの使用アクティビティに対する請求金額、ある使用情報が記録されたか並びに／又は格納場所及び／又はコンテンツプロバイダに入手可能であるかどうかに基づく請求金額の相違、このようなコンテンツに関連する再配布の権利、監査伝送の報告頻度、このようなコンテンツの使用に関連する何らかの料金を支払うために用いられ得るクレジット及び／又は通貨の形態、ある量の使用に関連するディスカウント、同一の及び／又は異なるコンテンツプロバイダからの他のコンテンツに関連する権利の存在によって入手可能なディスカウント、販売、など。さらに、VDEコンテンツカタログ3322は、コンテンツを利用するために必要とされるコンポーネントアセンブリの一部または全体を示し得る。コンテンツは、エンドユーザのシステムと格納場所とがメッセージを交換していずれの必要なVDEコンポーネントアセンブリ又は他のVDE制御情報もが識別され、さらに必要であり且つ承認されれば、（例えば上記アセンブリ又は情報がないということが、登録中及び／又は使用を試みているときに検出されて後に要求されるよりも）このようなコンテンツに沿ってエンドユーザに配送されることを保証することを補助できるように行われる。

本実施例において、VDE格納場所を利用するためには、エンドユーザは格納場所に登録しなければならない。著者の場合に上述したものと類似の様式で、VDEエンドユーザが自分自身のVDEインストレーションからネットワークを介して格納場所までメッセージを伝送し、エンドユーザが格納場所により提供されているサービス（例えば、格納場所に格納された及び／又は格納場所により参照されたコンテンツへアクセスする、格納場所により提供されているクレジットを使用するなど）を利用したいということを示す。このメッセージに応答して、格納場所のコンテンツシステム3302Aのユーザ／著者登録システムと情報交換所システム3302Bのユーザ／著者登録システムとが、エンドユーザからの情報に対する要求を

（例えば、オンラインで及び／又はバッチインタラクションにより）伝送する。コンテンツシステム3302Aのユーザ／著者登録システムにより要求された情報は

、ユーザがアクセスしたいコンテンツのタイプ、ユーザの電子機器600の特性などを含み得る。情報交換所システム3302Bのユーザ／著者登録システムにより要求された情報は、ユーザが情報交換所システム3302Bでクレジットアカウントを設立したいと望んでいるか否か、ユーザは課金目的のためにどのような他のクレジット形態を用いたいと望んでいるか、格納場所から得られたコンテンツとインタラクトする間にどのような他の情報交換所がエンドユーザによって用いられ得るか、使用分析情報の放出および取り扱いに対する好みに関してユーザが確立した如何なる一般的規則などをも含み得る。一旦エンドユーザが登録情報を完成させて格納場所に伝送すれば、格納場所はユーザのアカウントプロフィールを構築し得る。本実施例においては、このような要求およびレスポンスは、送信パーティおよび受信パーティの安全なVDEサブシステム間の安全なVDE通信により取り扱われる。

格納場所を利用するために、エンドユーザはアプリケーションソフトウェアを動作し得る。本実施例において、エンドユーザは、標準アプリケーションプログラム（例えば、MosaicなどのWorld Wide Webブラウザ）を利用してもよいし、又は登録プロセスが完了した後に格納場所によって提供されるアプリケーションソフトウェアを利用してもよい。エンドユーザが格納場所によって提供されるアプリケーションソフトウェアを利用することを選択する場合、標準パッケージが用いられた場合に起こり得るインタラクションのある種の複雑さを回避することができることがあり得る。標準パッケージは、比較的使い易いことがしばしばあるが、VDE認識機能を組み込んだカスタマイズされたパッケージは、ユーザにとってより使い易いインターフェースを提供し得る。さらに、サービスの使用を簡素化するために、格納場所のある種の特性がインターフェースに組み込まれ得る（例えば、America Onlineにより提供されるアプリケーションプログラムに類似している）。

エンドユーザは、ネットワークを用いて格納場所に接続し得る。本実施例においては、ユーザが格納場所に接続した後、認証プロセスが起こる。このプロセスは、（例えば、ログインおよびパスワードプロトコルの使用を介して）ユーザ

によって行われるか、又はVDE認証において格納場所の電子機器とインタラクトするエンドユーザの電子機器の安全なサブシステムによって確立されるかのいずれかによってなされ得る。いずれの場合も、格納場所とユーザとは、まず初めに正しい他のパーティと接続していることを確認しなければならない。本実施例においては、安全な状態になった情報が両パーティ間に流れると、VDEの安全な認証が起こらなければならず且つ安全なセッションが確立されなければならない。一方、交換されるべき情報がすでに安全な状態になっている及び／又は認証なしに入手可能である場合（例えば、ある種のカタログ情報、すでに暗号化されており特別な取り扱いを必要としないコンテナなど）は、「より弱い」形態のログイン／パスワードが用いられ得る。

一旦エンドユーザがVDE格納場所に接続して認証が起これば、ユーザは、ユーザインターフェースソフトウェアを操作して、格納場所のコンテンツカタログ3322（例えば、刊行物、ソフトウェア、ゲーム、映画などのリスト）をブラウズし、サーチ機構の助けを借りて興味のあるコンテンツを探し出し、コンテンツの配送の予定を立て、アカウント状況、使用分析情報の入手可能性、課金情報、登録およびアカウントプロフィール情報などを問い合わせる。ユーザがコンテンツを獲得するために接続している場合、そのコンテンツの使用条件がユーザに配送され得る。ユーザが格納場所に使用情報を配送するために接続している場合、その伝送に関する情報がユーザに配送され得る。これらのプロセスのうちのいくつかを以下により詳細に記載する。

本実施例において、エンドユーザがVDE格納場所から（例えば入手可能なオプションのメニューから選択することにより）コンテンツを要求すると、コンテンツシステム3302Aは、コンテンツリファレンス及び／又はコンテンツ格納部のいずれか内にコンテンツを探し出す。その後コンテンツシステム3302Aは、コンテンツカタログ3322、エンドユーザのアカウントプロフィール、及び／又は著者のアカウントプロフィール内に格納された情報を参照することにより、エンドユーザの要求を満たすためのVDEコンテンツコンテナを作成するために必要であり得るコンテナフォーマット及び／又は制御情報の厳密な性質を決定する。その後送

出システムが情報交換所システム3302Bにアクセスすることにより、コンテナに含むべきいかなる追加の制御ストラクチャをも収集し、コンテンツをエンドユーザに配送することに関連する取り引きか、取り引きがプロセスされ得るか否かのいずれかに影響を与え得る著者及び／又はエンドユーザのアカウントプロフィールの特徴を決定する。取り引きが承認されてコンテナに必要な全てのエレメントが入手可能である場合、制御パッケージャがエンドユーザによる要求に適した制御情報のパッケージを形成し、コンテナパッケージャがこの制御情報のパッケージとコンテンツとを取って適切なコンテンツ（コンテナと共に配送可能であり得る許可を含む、いずれの暗号化条件をも組み込んでいる、など）を形成する。格納場所または著者のアカウントプロフィールにより必要とされた場合、コンテンツの配送に関連する取り引きは、送出システムの取り引きシステムにより記録される。コンテナ、および配送に関連する何らかの取り引きが完了すると、コンテナはネットワークを介してエンドユーザに伝送される。

エンドユーザは、格納場所から受け取るVDEコンテンツの使用に関連する請求金額を支払うために、エンドユーザの、VDEをインストールした安全なサブシステム内に安全に格納されたクレジット及び／又は通貨を利用し得る。そして／又はユーザは、エンドユーザによって上記コンテンツの受け取りのために支払いが行われる「仮想」格納場所を含む遠隔の格納場所に、安全なクレジット及び／又は通貨アカウントを維持し得る。後者のアプローチは、エンドユーザがHPEベースの安全なサブシステムしか有していない場合に特に、格納場所及び／又はコンテンツプロバイダへの支払いに対してより大きな保証を提供する。本実施例において、エンドユーザの電子クレジット及び／又は通貨アカウントが格納場所に維持されている場合、エンドユーザが格納場所からコンテンツを受け取ることに基づいて、上記アカウントに請求が行われる。このような遠隔のエンドユーザアカウントに対する更なる請求は、受け取られたコンテンツのエンドユーザによる使用に基づいて、および格納場所の情報交換所システム3302Bへ通信されるコンテンツ使用情報に基づいて行われ得る。

本実施例において、エンドユーザが（格納場所の使用を介してコンテンツが獲得され得るコンテンツプロバイダが、プロバイダのコンテンツに関連する使用料

金を支払うために通貨及び／又はクレジットを利用することを、承認している）金融プロバイダとの関係を確立していない場合、そして／又はエンドユーザがこのようなクレジットの新しい源を欲している場合、エンドユーザは格納場所の情報交換所システム3302Bからのクレジットを要求し得る。エンドユーザがクレジットを認められた場合、格納場所は、格納場所により管理される予算メソッドに関連するクレジット額（例えば、１以上のUDEに記録される）という形態でクレジットを認める。定期的に、このような予算メソッドに関連する使用情報がエンドユーザにより格納場所の監査システムに伝送される。このような伝送の後（しかし可能性としては接続が断たれる前に）、課金システムによる処理のためにクレジット額が記録され、格納場所のビジネス慣習に応じて、エンドユーザにより使用可能なクレジット額が同一のまたはそれに続く伝送で補充され得る。本実施例において、格納場所の情報交換所は、メールを介してクレジット額を回収するペーパーシステムによる課金システムと、1以上のクレジットカードに請求することによりクレジット額を回収するクレジットカードシステムと、銀行口座から直接引き落とすことによりクレジット額を回収する電子基金送金システムとをサポートする。格納場所は、類似の手段を用いることにより、著者に借りている金額に対して分配システムにより決定された支払いを自動的に行い得る。監査プロセスに関する更なる詳細を以下に述べる。

上記のように、本実施例におけるエンドユーザ3310は、定期的にVDE格納場所にコンタクトすることにより、コンテンツ使用情報（例えば、予算の消費、他の使用アクティビティの記録などに関する）を伝送し、予算を補充し、アカウントプロフィールを改変し、使用分析情報にアクセスし、そして他の管理および情報交換アクティビティを行う。場合によっては、エンドユーザが更なる制御ストラクチャを得るために格納場所にコンタクトしたいと望むことがあり得る。例えば、エンドユーザが格納場所からVDEコンテンツコンテナを要求して獲得した場合、そのコンテナは典型的にはコンテンツ、著者の条件とアカウントプロフィール、エンドユーザのアカウントプロフィール、コンテンツカタログ3322、及び／又は配送の環境に適した制御ストラクチャに沿ってエンドユーザに送出される（配送の環境とは、例えば、特定の著者からの初めての配送、定期購読、販売促進、

あ

る種の広告マテリアルの存在及び／又は不在、ユーザのローカルVDEインスタンスによりユーザのために形成された要求などである）。本実施例においては、格納場所が全ての関連する制御ストラクチャを配送しようと試みたことがあり得たとしても、いくつかのコンテナはエンドユーザが行うことを予期していなかった（そして他の基準もコンテナに含むことを自動的に選択しなかった）がそれにもかかわらずエンドユーザが行いたいと望むオプションを加える余裕のある制御ストラクチャを含み得る。この場合、エンドユーザは格納場所にコンタクトして、このようなオプション下でコンテンツを利用するために必要な追加の制御情報（例えば制御ストラクチャを含む）要求したいと望み得る。

例えば、エンドユーザが全体的な制御ストラクチャ、すなわち、あるタイプのアクセスがコンテナに対して行われた回数とこのようなアクセスに対する基本的な使用料金とを記録するというオプションを含む全体的な制御ストラクチャを有するVDEコンテンツコンテナを獲得し、全体的な制御ストラクチャ内の別のオプションによってエンドユーザが特定のコンテナへのアクセスに対する支払いを、コンテナのコンテンツを用いて、費やした時間に基づいて行うことが可能となり、さらにエンドユーザが後者の形態の使用をサポートする制御を元々受けとらなかった場合、格納場所はこのような制御を、後に、すなわちユーザが要求したときに配送し得る。別の実施例においては、著者は、ユーザが変更された制御ストラクチャを有するコンテンツコンテナを用いるために受け取り得るか又は受け取らなければならない制御ストラクチャを（例えば、販売、新しいディスカウントモデル、改変されたビジネス戦略などを反映させるために）変更したことがあり得る。例えば、あるVDEコンテンツコンテナに関連する1以上の制御ストラクチャが、このようなストラクチャを引き続いて承認するための「リフレッシュ」を必要とすることがあり得るし、または制御ストラクチャの期限が切れることがあり得る。このことは（所望であれば）、VDEコンテンツプロバイダが、エンドユーザのサイトで（ローカルなVDEの安全なサブシステムを用いて）定期的にVDE制御情報を改変及び／又は追加することを可能にする。

本実施例の（格納場所から受け取られたコンテンツの使用に関する）監査情報は、情報交換所のレシートシステム3362によりエンドユーザ3310から安全に受け取られる。上記のように、このシステムは、監査情報を処理し、このような処理のアウトプットの一部または全部を課金システムへ送り、及び／又はこのようなアウトプットを適切なコンテンツ著者に伝送し得る。このような監査情報の送信は、情報取り扱い技術を報告する安全なVDE通路を用いる。監査情報はまた、エンドユーザ、格納場所、第三のパーティであるマーケットリサーチャ、及び／又は1以上の著者による使用のための、エンドユーザコンテンツの使用の分析結果を生成するために、分析システムに送られ得る。分析結果は、単一の監査伝送、監査伝送の一部、単一のエンドユーザ及び／又は複数のエンドユーザ3310からの監査伝送の集まり、または分析の対象（例えば、与えられたコンテンツエレメントまたはエレメントの集まりの使用パターン、あるカテゴリのコンテンツの使用、支払い履歴、人口統計的使用パターンなど）に基づいた監査伝送のある種の組み合わせに基づき得る。エンドユーザに情報を送って、例えば予算を補充するため、使用制御を配送するため、許可情報を更新するため、および情報交換所とのインタラクションの間にエンドユーザによって要求された及び／又は必要とされたある種の他の情報及び／又はメッセージを伝送するために、レスポンスシステム3364が用いられる。エンドユーザが情報交換所に接続して伝送する間に、ある種の取り引き（例えば、時間、日付、並びに／又は接続及び／又は伝送の目的）が、監査システムの取り引きシステムによって記録され、それによって格納場所及び／又は著者の必要条件を反映させる。

ある種の監査情報は、著者に伝送され得る。例えば、著者3306Aは、エンドユーザから集められたある種の情報が監査システムによって処理されることなく著者3306Aに伝送することを必要とすることがあり得る。この場合、伝送の事実は監査システムによって記録されるが、著者3306Aは格納場所がこの情報にアクセスすること、情報を処理すること、及び／又は情報を用いることを許可しないで（または許可することに加えて）著者自身の使用分析を行うことを選択したということがあり得る。本実施例において、格納場所は、1以上のエンドユーザ3310

から受け取られて、著者3306Aによって提供されたコンテンツをこのようなユーザが使用したことに関する料金の支払いにより生成された、格納場所の予算に関連する使用情報の一部を、著者3306Aに提供し得る。この場合、著者3306Aは、コンテンツに関連するある種の使用情報と、コンテンツに対する格納場所の予算に関する使用情報とを比較することにより、使用パターンを分析する（例えば、料金の面での使用を分析する、可能性のある詐欺を検出する、ユーザのプロフィール情報を生成するなど）ことができる。著者3306Aのコンテンツに関連して著者3306Aに支払われるべき、情報交換所により収集される使用料金は、情報交換所の分配システムによって決定される。分配システムは、このような決定の結果生じる著者3306Aへの支払いに関する使用情報を（完全な又は要約形態で）含み得る。このような支払いおよび情報のレポートは、エンドユーザのVDEの安全なサブシステムから情報交換所の安全なサブシステム、さらに著者の安全なサブシステムにつながるVDE通路内で起こる、完全に自動化されたプロセスシークエンスであり得る。

本実施例において、エンドユーザ3310は、VDE許可及び／又は他の制御情報を格納場所3302に伝送して、分析システムにより使用される監査システムによって収集される使用情報へのアクセスを許可及び／又は禁止する。このことは、部分的に、このような情報の使用に関連する場合のエンドユーザのプライバシー権利を保証することを補助し得る。いくつかのコンテナは、制御ストラクチャの一局面として、使用情報を分析の目的のためにエンドユーザにとって入手可能にすることを必要とし得る。他のコンテナは、エンドユーザに、使用情報が分析のために使用されることを許可するか、このような情報のこのような使用を部分的にまたは全体的に禁止するかのオプションを与える。何人かのユーザは、ある種の情報の分析を許可して他の情報に対する許可を禁止することを選択し得る。本実施例において、エンドユーザ3310は、例えば、分析の目的のために使用され得る情報の細分性を制限することを選択し得る（例えば、エンドユーザが、ある期間に見られた映画の数の分析は許可するが特定の映画の使用は許可しないということがあり得る、エンドユーザが、人工統計分析のためのZIPコードの放出は許可す

るが氏名および住所などの使用は許可しないということがあり得る、などである）。著者及び／又は格納場所3302は、例えば、エンドユーザが分析の目的のためにある種の使用情報を放出することに同意した場合、エンドユーザ3310により低い料金を課すことを選択し得る。

本実施例において、格納場所3302は、１人より多い著者により作成されたコンテンツを受け取り得る。例えば、著者Ｂ、著者Ｃ、および著者Ｄが各々、単一のコンテナ内でエンドユーザ3310に配送されるコンテンツの一部分を作成することがあり得る。例えば、著者Ｂがリファレンスワークを作成し、著者Ｃが著者Ｂのリファレンスワークに対するコメントを作成し、著者Ｄが著者Ｂのリファレンスワークと著者Ｃのコメントとに対する１セットのイラストを作成するということがあり得る。著者Ｂが、著者Ｃと著者Ｄのコンテンツをまとめて更なるコンテンツ（例えば、上記のリファレンスワーク）を追加し、そのようなコンテンツを単一のコンテナに入れて、上記単一のコンテナが格納場所3302に伝送されるということがあり得る。これに代えて、各々の著者が自分自身のワークを別々に格納場所3302に伝送してもよい。その場合、コンテナをエンドユーザに送出する前に著者のそれぞれのワークを組み合わせるためにテンプレートが用いられるべきであることを指示しておく。さらにこれに代えて、全体のコンテンツストラクチャを反映するコンテナが格納場所3302に伝送されて、コンテンツの一部または全部が、コンテンツ格納部内に格納されるために格納場所3302に配送されるのではなく、コンテンツリファレンス内で参照されることがあり得る。

エンドユーザがコンテナコンテンツを利用するとき、コンテンツ使用情報は、例えば、少なくとも部分的にはそのセグメントを作成した著者に基づいて使用情報を系統立てる制御ストラクチャに応じて分離され得る。これに代えて、著者及び／又はVDE格納場所3302は、VDE制御情報に応じて使用情報を安全に分割及び／又は共有する１以上の他の技術をネゴシエートし得る。さらに、コンテナに関連する制御ストラクチャは、コンテナの特定の部分の使用、コンテナ全体の使用、使用する特定のページ、または著者によってネゴシエートされた（又は同意された）他の機構に基づいて、コンテンツの一部分に関連する使用料金を異ならせる

モデルを実行し得る。使用情報、分析結果、分配、および他の情報交換所プロセスのレポートはまた、このようなプロセスに関して、格納場所3302の参加者（著者、エンドユーザ3310、及び／又は格納場所3302）が達した同意内容を反映する様式で、生成され得る。これらの同意内容は、これらの参加者間のVDE制御情報ネゴシエーションの結果であり得る。

本実施例において、１つのタイプの著者は、パブリッシャ3308である。本実施例において、パブリッシャ3308は、「内部の」ネットワークを介して、VDEベースのローカル格納場所3302と通信し、上記のネットワークを介して公的な格納場所3302と通信する。パブリッシャ3308は、「内部の」ネットワークへのアクセスを有する他の参加者により使用されるローカル格納場所3302に配送されるコンテンツ及び／又はVDE制御ストラクチャテンプレートを作成または提供し得る。これらのテンプレートは、コンテナのストラクチャを記述するために用いられ得、さらにパブリッシャ3308の組織内の誰に、格納場所3302への配送される（及び／又は格納場所3302により参照される）刊行物に関連する、組織内で作成されたコンテンツに関して、どのような行為をなし得るかを記述し得る。例えば、パブリッシャ3308は、定期刊行物がコンテンツのストラクチャと含まれ得る情報のタイプ（例えば、テキスト、グラフィクス、マルチメディア表現、広告など）、コンテンツの相対的ロケーション及び／又は提示の順序、あるセグメントの長さなどに関して、あるフォーマットを有すると決定（且つ上記テンプレートの使用により制御）し得る。さらに、パブリッシャ3308は、例えば、刊行物のエディタがコンテナへの書き込みを許可し得る唯一のパーティであること、および組織の司書がコンテンツにインデックス及び／又はアブストラクトを付し得る唯一のパーティであることを（適切な許可の配布を介して）決定し得る。さらに、パブリッシャ3308は、例えば、ある１以上のパーティのみがコンテナを、格納場所3302へ配送するために入手可能な形態で最終的なものにすることを許可し得る（例えば、上記許可は、格納場所のエンドユーザ3310に関連する次の配布アクティビティを行うために格納場所3302が必要とし得る、配布許可を含む許可のタイプに対する制御を維持することにより行われる）。

本実施例において、著者3306Eは、パブリッシャ3308に直接接続しており、パブリッシャ3308が著者3306Eのコンテンツ用のコンテナの特徴を確立する著者用テンプレートを提供し得るようになっている。例えば、著者3306Eがパブリッシャ3308により配布される本を作成した場合、パブリッシャ3308は、著者3306E選択用の制御メソッドオプションを提供し、且つ著者3306Eのワークを安全に配布するためのVDE制御ストラクチャを提供する、VDE制御ストラクチャテンプレートを定義し得る。著者3306Eとパブリッシャ3308とは、著者3306Eが用いるテンプレート特性、特定の制御ストラクチャ、及び／又はパラメータデータのためのVDEネゴシエーションを採用し得る。著者3306Eは、その後コンテンツコンテナ用の制御ストラクチャを作成するテンプレートを用い得る。パブリッシャ3308は、その後、著者3306Eとパブリッシャ3308との間の電子契約、ならびに格納場所3302とパブリッシャ3308との間の電子契約を含むVDE拡張契約下において、格納場所3302にこれらのワークを配送し得る。

本実施例において、パブリッシャ3308はまた、著者3306Eのワークをローカル格納場所3302にとって入手可能にし得る。エディタは、著者Fが刊行物のコンテンツの一部分を作成することを（例えば、適切な許可の配布により）承認する。本実施例において、エディタは、著者Fのワークを検討及び／又は改変し得、さらにそれを著者3306Eにより提供されたコンテンツを有するコンテナ（ローカル格納場所3302で入手可能である）内に含み得る。エディタは、著者3306Eのコンテンツを改変することをパブリッシャ3308から許可されている場合もあるし、許可されていない場合もある（許可されるかされないかは、パブリッシャ3308と著者3306Eとの間に起こり得たネゴシエーション、および著者3306Eのコンテンツを改変する許可がパブリッシャ3308により再配布可能な形態で保持されている場合に、このような権利をエディタまで拡張しようというパブリッシャ3308の決定に依存する）。エディタはまた、(a)著者がコンテナに直接書き込むことを許可するプロセスを用いること、及び／又は(b)含有のためにローカル格納場所3302からコンテナを検索することにより、他の著者からのコンテンツを含み得る。ローカル格納場所3302はまた、パブリッシャ3308の組織により用いられた他のマテリ

アル（例えば、データベース、他のリファレンスワーク、内部ドキュメント、検討用ドラフトワーク、トレーニングビデオなど）用にも用いられ得る。このようなマテリアルは、適切な許可を与えられれば、エディタにより作成されたコンテンツのVDEコンテナコレクション内で採用され得る。

本実施例において、司書は、反転されたインデックス、（例えば制限されたボキャブラリからの）キーワードリスト、コンテンツのアブストラクト、改訂の履歴などを作成及び／又は編集する責任を有する。パブリッシャ3308は、例えば、

このタイプのコンテンツを作成する許可を司書のみに与える得る。パブリッシャ3308はさらに、この作成及び／又は編集が格納場所3302へのコンテンツの放出前に起こることを必要とし得る。

実施例－－VDE管理コンテンツおよび制御情報の進化および変形

VDEコンテンツ制御アーキテクチャは、コンテンツ制御情報（コンテンツ使用を支配する制御情報など）が複数のパーティのVDE制御情報必要条件に準拠するように整形されることを可能にする。このような複数のパーティのコンテンツ制御情報を形成することは、通常、コンテンツ取り扱いおよび制御モデルにおいて役割を果たすパーティ（例えば、コンテンツクリエータ、プロバイダ、ユーザ、情報交換所など）により安全に寄与された制御情報から安全に制御情報を引き出すことを含む。別々に管理されたVDEコンテンツの複数のピースを組み合わせて単一のVDEコンテナオブジェクトにするためには（特に、このような別々に管理されたコンテンツピースが、異なる、例えば相反するコンテンツ制御情報を有する場合には）、複数のパーティの制御情報が必要になり得る。VDE管理コンテンツピースをこのように安全に組み合わせるためには、それぞれのVDE管理コンテンツピースの、いずれの組み合わせに関する規則をも含む、制御情報必要条件を満たし、且つこのような複数の制御情報セット間の容認可能な一致を反映するコンテンツ制御条件を安全に引き出す、VDEの能力を必要とすることが頻繁にある

VDE管理コンテンツピースの組み合わせの結果、VDE管理コンテンツ複合体が生成され得る。VDE管理コンテンツは、上記コンテンツピースに関連するコンテン

ツ管理情報に応じて実行され且つ１以上の安全なVDEサブシステムPPE650の使用を介して処理されなければならない。様々なVDEコンテンツピースを有する組み合わせプロダクトを作成するために、VDE管理コンテンツピースを埋め込むこと又は組み合わせることをサポートするVDEの能力は、VDEコンテンツプロバイダがVDE電子コンテンツプロダクトを最適化することを可能にする。VDE管理コンテンツピースの組み合わせの結果、統合されたコンテンツ及び／又は同時に生じる、別々の、ネスティングされたVDEコンテンツコンテナを「保持する」VDEコンテンツコンテナが生成され得る。

以前は別々に管理されていたVDEコンテンツ部分の異なるピースを保持するコンテンツコンテナを作成する、VDEの能力は、VDEコンテンツプロバイダがプロダクトを開発することを可能にする。上記プロダクトのコンテンツ制御情報は、コンテンツピースのプロバイダの目的と一致し、且つ、商用配布用プロダクトとしてあるコンテンツ組み合わせ物を作成し得るコンテンツ統合者の目的とも一致する、価値に関する提案を反映している。例えば、あるコンテンツプロバイダによって商用チャネル（ネットワーク格納場所など）に「送り出された」コンテンツプロダクトは、異なるコンテンツプロバイダ及び／又はエンドユーザによってVDEコンテンツコンテナに組み込まれ得る（このような組み込みが送り出されたプロダクトのコンテンツ制御情報によって許可される限り）。これらの異なるコンテンツプロバイダ及び／又はエンドユーザは、例えば、このようなコンテンツの使用を規制する異なる制御情報を提出し得る。これらの異なるコンテンツプロバイダ及び／又はエンドユーザはまた、適切な承認を与えられれば、送り出されたコンテンツのある部分と他のパーティから受け取った（及び／又は自分自身で作成した）コンテンツとを異なる様式で組み合わせて異なるコンテンツコレクションを作成し得る。

このようにVDEは、VDE管理コンテンツの与えられたピースのコピーが安全に組み合わされて異なるコンテンツ統合物になることを可能にする。上記統合物の各々は、異なるVDEコンテンツ統合者のプロダクト戦略を反映する。VDEのコンテンツ統合能力の結果、広範囲の互いに競合する電子コンテンツが作成される。上記

互いに競合する電子コンテンツは、異なるコンテンツコレクション全体を提供し、このような複数のプロダクトに共通し得るコンテンツ用の異なるコンテンツ制御情報を採用し得る。重要なことは、VDEは安全に且つフレキシブルに、VDEコンテンツコンテナ内のコンテンツを編集すること、VDEコンテンツコンテナからコンテンツを抽出すること、VDEコンテンツコンテナにコンテンツを埋め込むこと、およびVDEコンテンツコンテナのコンテンツ複合物を整形および再整形することをサポートするということである。このような能力は、VDEサポートプロダクトモデルが電子商用モデル内の「次の」参加者の必要条件を次々と反映させることにより進化することを可能にする。その結果、与えられたVDE管理コンテンツが、取り扱いおよび分岐の通路を移動するときに、多くの異なるコンテンツコンテナおよびコンテンツ制御情報商用モデルに参加し得る。

VDEコンテンツおよび上記コンテンツに関連する電子契約は、非電子プロダクト用の従来のビジネス慣習を反映する商業的方法において採用され且つ次々と操作され得る（VDEは、このような従来のモデルの大半に比べて、より高いフレキシビリティおよび効率性をサポートするが）。VDE制御情報は、コンテンツクリエータ、他のプロバイダ、並びに取り扱いおよび制御参加者という他の通路により採用されたVDE制御情報によってのみ制限されて、電子コンテンツプロダクトモデルの「自然な」且つ妨害されない流れおよび上記モデルの作成を可能にする。VDEは、VDEプロダクトおよびサービスのこの流れを、仮想配布環境内でコンテンツの組み合わせ、抽出、および編集を介してプロダクト複合物をうまく且つ安全に整形および再整形するクリエータ、プロバイダおよびユーザのネットワークを介して、提供する。

VDEは、異なる時に、異なる源により、及び／又は異なるコンテンツタイプを表すように提供されたコンテンツを安全に組み合わせる手段を提供する。これらのコンテンツのタイプ、タイミング、及び／又は異なる源は、VDEコンテンツコンテナ内において複雑なコンテンツアレイを形成するために採用され得る。例えば、VDEコンテンツコンテナは、複数の異なるコンテンツコンテナオブジェクトを含み得、上記コンテンツコンテナオブジェクトの各々は、使用が少なくとも部

分的に所有者のVDEコンテンツ制御情報セットによって制御され得る、異なるコンテンツを含む。

VDEコンテンツコンテナオブジェクトは、安全なVDEサブシステムの使用を介して、「ペアレント」VDEコンテンツコンテナ内に「無事に」埋め込まれ得る。この埋め込みプロセスは、埋め込まれたオブジェクトの作成、または以前は別々であって現在埋め込まれているオブジェクトを、少なくとも上記オブジェクトをそのロケーションとして適切に参照することによりVDEコンテンツコンテナ内に含めることを含む。

ペアレントVDEコンテンツコンテナ内に埋め込まれたコンテンツオブジェクトは、

（１）VDE安全サブシステムPPE650内で、１つ以上のVDEコンポーネントアセンブリの安全な処理によって独立オブジェクトから埋め込まれたオブジェクトへと安全に変換することによりペアレントVDEコンテンツコンテナに埋め込まれた、以前に作成されたVDEコンテンツコンテナでありうる。この場合、埋め込まれたオブジェクトは、ペアレントコンテナに関連する１つ以上のパーミッションレコードを含むコンテンツ制御情報に供されうるが、例えば、コンテンツ識別情報とは別の固有のコンテンツ制御情報を有していない場合もあり、あるいは、その埋め込まれたオブジェクトが、固有のコンテンツ制御情報（例えば、パーミッションレコード）によってより重点的に制御されてもよい。

（２）別のVDEコンテンツコンテナから（コンテンツ制御情報とともに）、埋め込まれたVDEコンテンツコンテナオブジェクトの形態で、ペアレントVDEコンテンツコンテナへの内包に適用できうるように抽出したコンテンツを含みうる。この場合、抽出および埋め込みは、VDE安全サブシステムPPE650内で安全に実行され、かつ、所望のコンテンツをソースVDEコンテンツコンテナから取り出して（あるいはコピーして）、そのようなコンテンツを、そのどちらかがペアレントVDEコンテンツコンテナに埋め込まれうる、あるいは埋め込まれるようになりうる新しいまたは既存のコンテナオブジェクトに配置し得る、１つ以上のVDE処理を用いて行いうる。

（３）まず作成され、その後VDEコンテンツコンテナオブジェクトに配置されたコンテンツを含みうる。この受容コンテナは、すでにペアレントVDEコンテンツコンテナに埋め込まれている場合があり、そして他のコンテンツをすでに含んでいる場合がある。そのようなコンテンツが配置されるコンテナは、コンテンツとインタラクトするVDEを意識しているアプリケーションと、そのようなVDEコンテナを安全に作成し、かつそのようなコンテナをデスティネーションであるペアレントコンテナに安全に埋め込んだ後にそのようなコンテンツをVDEコンテナに配置する安全なVDEサブシステムとを用いて指定されうる。あるいは、コンテンツは、VDEを意識しているアプリケーションを使用せずに指定され、その後、VDEコンテンツコンテナへのコンテンツの移動を管理するために、VDEを意識しているアプリケーションを用いて操作されうる。そのようなアプリケーションは、VDEを意識しているワードプロセッサ、デスクトップおよび／またはマルチメディアパブリッシングパッケージ、グラフィックスおよび／またはプレゼンテーションパッケージ等でありうる。また、そのようなアプリケーションは、オペレーティングシステム機能（例えば、VDEを意識しているオペレーティングシステムまたはMicrosoft Windowsと互換性のあるパッケージングアプリケーションのようなO/Sとともに作動するミニアプリケーション）であり得、VDEの「外」からVDEオブジェクトの内部へのコンテンツの移動は、例えば、マウスなどのポインティングデバイスを用いてファイルをVDEコンテナオブジェクトに「ドラッギング」することに伴う「ドラッグとドロップ」のメタファーに基づきうる。あるいは、ユーザがコンテンツの一部を「カット」し、最初にコンテンツを「クリップボード」に配置し、その後、目標コンテンツオブジェクトを選択して、そのコンテンツをそのようなオブジェクトにペーストすることによって、そのような部分をVDEコンテナに「ペースト」しうる。このような処理により、VDEコンテンツ制御情報の管理およびVDE安全サブシステムの制御の下、そのコンテンツを目標オブジェクトにおけるある位置、例えばオブジェクトの最後、またはフィールド識別子などのコンテンツによって、あるいはそのコンテンツとともに運ばれる識別子に対応するオブジェクトの一部に、自動的にコンテンツを配置し得、あるいは、そ

の埋め込み処理により、目標オブジェクトのコンテンツおよび／またはコンテンツのテーブルおよび／または他のディレクトリ、インデックス等をユーザが走査検索できるユーザインタフェースがポップアップされうる。このような処理はさらに、このような埋め込まれたコンテンツに適用されるVDEコンテンツ制御情報に関する特定の決定（予算の制限使用、レポーティング通路、使用登録要件など）をユーザが下すことを可能にし得、および／またはコンテンツを埋め込む特定の位置を選択することに伴い、このような処理は全て、実用的に適用される程度にトランスペアレントに行われなければならない。

（４）オブジェクトの埋め込みおよびリンクのための１つ以上のオペレーティングシステムユーティリティ、例えばMicrosoft OLE規格に準じたユーティリティと連係してアクセスされうる。この場合、VDEコンテナは、OLE「リンク」と関連しうる。VDE保護されたコンテナへのアクセス（VDE保護されたコンテナからのコンテンツの読み出しおよびそのコンテナへのコンテンツの書き込みを含む）は、OLEを意識しているアプリケーションから、保護されたコンテンツと関連する制御情報と連係してその保護されたコンテンツにアクセスするVDEを意識しているOLEアプリケーションへと渡されうる。

VDEを意識しているアプリケーションはまた、PPE内で、コンポーネントアセンブリとインタラクトし得、これによって、コンテンツがペアレントまたは埋め込まれたVDEコンテンツコンテナのどちらにある場合でも、VDEコンテナのコンテンツの直接編集が可能となる。これは、例えばVDEコンテナのコンテンツを直接編集する（追加、削除、または改変する）ためのVDEを意識しているワードプロセッサの使用を含みうる。VDEコンテナコンテンツの編集の基礎を成す安全なVDE処理は、編集者（ユーザ）にとって大部分あるいは完全にトランスペアレントであり得、トランスペアレントに、編集者がVDEコンテンツコンテナ階層のコンテンツのいくつか、あるいは全てを（VDEを意識しているアプリケーションを用いて）安全に走査検索でき、かつ、VDEコンテンツコンテナ階層に埋め込まれたVDEコンテンツコンテナのうちの１つ以上を安全に改変することができうる。

全てのVDE埋め込みコンテンツコンテナの埋め込み処理は通常、埋め込まれた

コンテンツに対する適切なコンテンツ制御情報を安全に識別することに伴う。例えば、VDEインストレーションおよび／またはVDEコンテンツコンテナ用のVDEコンテンツ制御情報を、安全かつ埋め込み者（ユーザ）にトランスペアレントに、コンテナの予め「適所」にあるコンテンツの１つ以上の部分（例えばすべての部分を含む）に適用されるように、同一のコンテンツ制御情報を、編集された（例えば、改変された、または追加された）コンテナコンテンツに適用しうる、および／または、制御セット間のVDE制御情報ネゴシエーションによって生成された制御情報を安全に適用する、および／または、そのコンテンツに以前に適用された制御情報を適用しうる。制御情報の適用は、編集されたコンテンツがペアレントまたは埋め込まれたコンテナのどちらにあるかとは無関係に起こり得る。安全にコンテンツ制御情報を適用する（このコンテンツ制御情報は、自動的および／または気付かれずに適用され得る）この同じ機能は、VDEコンテナオブジェクトのコンテンツの抽出および埋め込みによって、すなわちVDEコンテナオブジェクトの移動、またはコピーおよび埋め込みによってVDEコンテナに埋め込まれたコンテンツにも用いられうる。コンテンツ制御情報の適用は通常、１つ以上のVDE安全サブシステムPPE650内で安全に行われる。この処理は、使い易いGUIユーザインタフェースツールによって、ユーザが、特定の、または全ての埋め込まれたコンテンツに対してVDEコンテンツ制御情報を指定することができるVDEテンプレートを用いてもよく、異なる制御機能を絵で示す（記号化する）異なるアイコンによって表され得、かつ、そのような機能を、オブジェクトディレクトリ表示にリストされた埋め込まれたオブジェクトなどの、VDE保護されたコンテンツの増分に適用しうる代替の制御メソッドの中から（例えば、異なる計量の形態間で）選択するなどの、メニュー方式の、ユーザが選択できる、および／または、限定できるオプションを含みうる。

VDEコンテンツコンテナからコンテンツを抽出する、または、VDEを意識しているアプリケーションを用いて、VDEコンテンツを編集する、あるいはVDEコンテンツを作成することにより、ペアレントVDEコンテナに埋め込まれる新しいVDEコンテンツコンテナオブジェクト内に配置され得るコンテンツが提供される。あるい

は、そのようなコンテンツは、既存のコンテンツコンテナに直接配置されてもよい。これらの処理はすべて、１つ以上のVDEインストレーション安全サブシステム内で、VDEコンテンツ制御情報を処理することによって管理されうる。

VDEコンテンツコンテナオブジェクトは、埋め込まれたオブジェクトの位置および／またはコンテンツを解明するペアレントオブジェクトパーミッションレコードによって参照される制御情報によって、ペアレントオブジェクトに埋め込まれてもよい。この場合、埋め込まれたオブジェクトの既存のコンテンツ制御情報に対して、ほとんどあるいは全く改変がないことが要求されうる。あるVDEコンテンツコンテナに再配置されるVDEの安全に管理されたコンテンツは、例えば、再配置／埋め込み処理の間、暗号化されたあるいは保護された内容として（例えば、安全な不正改変不可能なバリア502によって）再配置されるコンテンツを維持し続けることが可能なVDEサブシステムの安全処理を用いることによって、再配置され得る。

埋め込まれたコンテンツ（および／またはコンテンツオブジェクト）は、異なる複数のパーティによって寄与される場合があり、１つ以上の安全なVDEサブシステムの使用によって安全に管理されたVDEコンテンツおよびコンテンツ制御情報一体化処理により、VDEコンテナに一体化しうる。この処理は、例えば、以下に記載の１つ以上の項目を含みうる。

（１）埋め込みおよび／またはその提示されたコンテンツの使用を制御する命令を安全に適用し、その命令は、少なくとも部分的にコンテンツプロバイダおよび／またはそのVDEコンテナのユーザによって適所に安全に配置された命令である。例えば、そのユーザおよび／またはプロバイダは、コンテンツの埋め込みの選択および／または制御オプション（例えば、VDEテンプレートの形で）を提供する１つ以上のユーザインタフェースとインタラクトしうる。そのようなオプションは、１つ以上の制御のうちどれが、コンテンツおよび／またはコンテンツ制御パラメータデータ（それ以前にはそのコンテンツが使用できない期間、コンテンツの使用コスト、および／またはソフトウェアプログラムの継続販売値引きなどの価格設定値下げ制御パラメータ）の入力の１つ以上の部分に適用されるべき

か、および／または、１つ以上の制御が前記の１つ以上の部分に適用されるべきか否かのオプションを含みうる。必須および／または任意のコンテンツ制御情報が、プロバイダおよび／またはユーザによって一旦確立されれば、それは、VDEコンテンツコンテナに埋め込まれる特定あるいは全てのコンテンツに、部分的あるいは完全に自動的に適用できうるコンテンツ制御情報として機能できる。

（２）受け取りVDEインストレーションのユーザと埋め込みのために提示されているコンテンツに関連するVDEコンテンツ制御情報との間のユーザインタフェースインタラクションの使用を含む、安全なVDEの管理されたネゴシエーション活動。例えば、そのような関連の制御情報は、あるコンテンツ情報を提案し得、コンテンツの受け手は、例えば、受け取る、複数から選択する、拒否する、代替の制御情報を提供する、および／または、あるコンテンツ制御情報の使用に条件を適用する（例えば、ある１人以上のユーザによってコンテンツが使用される場合に、および／または、あるコンテンツの使用量が、あるレベルを超えた場合に、

ある１つ以上の制御を受け取る）ことができる。

（３）受けとりVDEコンテンツコンテナおよび／またはVDEインストレーションのVDEコンテンツ制御情報と、提示されたコンテンツ（寄与されたVDEオブジェクトのパーミッションレコードにおける制御情報、あるコンポーネントアセンブリ、1つ以上のＵＤＥおよび／またはＭＤＥにおけるパラメータデータ等）に関連するコンテンツ制御情報に伴う、安全で自動化されたVDEの電子ネゴシエーションプロセス。

VDEコンテンツコンテナに埋め込まれたコンテンツは、下記（１）および／または（２）の形態で埋め込まれうる。

（１）新しいコンテナオブジェクトの形成を行わずに、VDEコンテンツコンテナ（このコンテナは、ペアレントまたは埋め込まれたコンテンツコンテナでもよい）の既存のコンテンツへと、直接的かつ安全に一体化されたコンテンツの形態。埋め込み後のコンテンツに関連するコンテンツ制御情報は、埋め込み後に必要とされる制御情報の確立を少なくとも部分的に制御する、前もって埋め込むどの

コンテンツ制御情報とも一貫性がなければならない。このように直接的に一体化された、埋め込まれたコンテンツに対するコンテンツ制御情報は、VDEコンテナ用の制御情報（例えば、コンテンツ制御情報を含む１つ以上のパーミッションレコード）に一体化されてもよく、および／または、その制御情報の一部を構成してもよい。

（２）VDEコンテンツコンテナオブジェクト内にネストされる１つ以上のオブジェクトにおいてコンテナに一体化されるコンテンツの形態。この場合、このコンテンツ用の制御情報は、ペアレントVDEコンテンツコンテナ用のコンテンツ制御情報によって運ばれてもよい。あるいは、この制御情報は、例えば、その中に含まれる、および／または、ネストされたVDEオブジェクトを含む１つ以上のコンテンツに特に関連した、１つ以上のパーミッションレコードによって、部分的に、または完全に運ばれうる。ペアレントVDEコンテンツコンテナ内にオブジェクトを含むVDEコンテンツのこのようなネスティングは、複数のレベルを用いてもよい。すなわち、VDEコンテンツコンテナにネストされたVDEコンテンツコンテナ自体が、１つ以上のネストされたVDEコンテンツコンテナを含んでもよい。

VDEコンテンツコンテナは、１つ以上のネストされたコンテナ（オブジェクト）を含むネスト化構造を有してもよい。この１つ以上のネストされたコンテナ（オブジェクト）はそれ自体が、コンテナ、および／または、１つ以上のタイプのコンテンツ、例えば、テキスト、画像、音声、および／またはその他のタイプの電子情報をさらに含みうる（オブジェクトコンテンツは、例えば記憶媒体上のバイトオフセット位置を参照するコンテンツ制御情報によって指定されうる）。このようなコンテンツは、ストリーム（動的に蓄積する、および／または流れる等の）形態で、および／または、静的（定義済みといった、固定された完全ファイル）な形態で、保存、通信、および／または、使用されうる。そのようなコンテンツは、１つ以上のVDEコンテンツコンテナのコンテンツのサブセットを抽出することによって得られうり、結果として生じる１つ以上のVDEコンテンツコンテナが直接作成される。VDEの安全に管理されたコンテンツは、（例えば、VDEを意識しているアプリケーション、または抽出能力を有するオペレーティングシステ

ムの使用によって）１つ以上のVDEコンテンツコンテナ内の１つ以上の位置のそれぞれから抽出を行うために識別され得、その後、安全サブシステムPPE650におけるVDE制御を実行するプロセスによって、新しいまたは現存するVDEコンテンツコンテナに安全に埋め込まれうる。このような抽出および埋め込み（VDE「エクスポーティング」）は、安全に実行することを含む、安全に保護を行うVDEエクスポーティングシステムを伴う。

VDEエクスポーティングおよび埋め込みに関係するVDE活動は、ある安全な形態から１つ以上の他の安全な形態へのVDEコンテンツの１つ以上の変換を行うことを伴う。このような変換は、変換されたコンテンツを新しいVDEコンテンツコンテナに移動させるとともに、または移動させることなしに行いうる（例えば、コンテンツの少なくとも１部分の使用を抑制するさらなるVDE処理なしに、このような変換処理の結果または他の出力を、保護されていない形態では明らかにしないPPE内で動作するコンポーネントアセンブリによって）。このような変換処理の一例は、その上で変換が行われたコンテンツ情報を全く保持しない、または、そのコンテンツ情報のある部分あるいは全部を保持する一方で、数学的変換を行うことと、数学的結果のような結果を生むこととを伴いうる。このような変換の

他の例としては、文書のフォーマットを変換する（例えば、Word PerfectからWindows用のWordのフォーマットへ、または、SGML文書からPostscript文書への変換）、ビデオフォーマットを改変する（例えば、QuickTimeビデオフォーマットからMPEGビデオフォーマットへの改変）、人工知能処理を行う（例えば、テキストを分析することによってサマリーレポートを作る）、および、他のVDE保護されたコンテンツからVDE保護されたコンテンツを得る他のプロセスを含む。

図79は、商用VDEユーザのアレンジメントの一例を示す。この例におけるユーザは、様々なメソッドでコンテンツを作成、配布、再配布、および使用する。この例は、コンテンツに関連する制御情報のある局面が、制御情報が処理および制御のチェーンを通して渡される際にどのように進化し得るかを示す。これらのVDEユーザおよび制御は、より詳細に以下に説明する。

この例におけるクリエーターＡは、VDEコンテナを作成し、（特に）VDE制御情

報の可能な「タイプ」の数例への参照を含む、関連のコンテンツ制御情報を提供する。この例を説明する一助とするために、別のVDE参加者に渡されたVDE制御情報のいくらかを、以下のより詳細な説明において、３つのカテゴリー、すなわち、配布制御情報、再配布制御情報、および使用制御情報にグループ化する。この例では、埋め込む制御情報の４番目のカテゴリーを、前述の３つのカテゴリー全てのエレメントとして考えることができる。制御情報の他のグループ化も可能である（VDEは、このメソッドで制御情報を組織化することを要求しない）。クリエーターＡによって作成されたコンテナのこの例に関連するコンテンツ制御情報は、図80に、Ｃ$_A$として示される。図80はさらに、クリエーターＡのVDEコンテンツコンテナに関係するイネーブルする制御情報を受けとり得るVDE参加者を示す。この例における制御情報のいくつかを、より詳細に以下に説明する。

クリエーターＡによって指定される配布制御情報のいくつか（本例では、配布者による制御情報の作成、改変、および／または使用に主に関連する制御情報）は、（ａ）配布者が、クリエーターＡに、コンテナのコンテンツの使用中ユーザのそれぞれに対して、ユーザ１人につき１ヶ月１０ドルの料金で報酬を支払うこと、（ｂ）配布者が、予算を補充することなしには、100人を超える独立ユーザがそのようなコンテンツにアクセスすることを許可し得ないように（例えば、コンテンツアクセス権を表す、100を超えるパーミッションレコードを作り得ないように）予算を組むこと、および、（ｃ）他の参加者への配布用に作成されたイネーブルする制御情報（例えば、パーミッションレコードおよび関連のコンポーネントアセンブリ）において、配布権が譲渡され得ないことを含む。

クリエーターＡによって指定されるコンテンツ再配布制御情報のいくつか（本例では、処理および制御のチェーンにおけるよりシニアな参加者によって許可される範囲内で配布者によって作成され、ユーザ／プロバイダ（本例では、ユーザ／配布者）に渡され、かつ、制御および／またはそのようなユーザ／配布者による再配布活動に関連する他の要件に関連する制御情報）は、（ａ）コンテンツアクセスをイネーブルする制御情報が、ユーザ／配布者によって、２レベルのみで再配布されうる要件を含み、そしてさらに、第１の再配布者が２レベルの再配布

に制限され、第１の再配布者がパーミッションを配送する相手である第２の再配布者は、１レベル追加された再配布に制限され、第２の再配布者からパーミッションを受け取るユーザはさらなる再配布を行うことができないような、各再配布が値を１つずつ減少することを必要とする（このような制限は、例えば、新しいパーミッションの作成に関連するVDE制御メソッドの１局面として、以下の１つ以上のメソッドを促す要件を含むことによって強制されうる。この１つ以上のメソッドは、（ｉ）１つ以上のメソッドに関連するUDEにおいて、例えば整数値として保存される再配布の現在のレベルを探しだし、（ii）再配布のレベル値を制限値と比較し、そして、（iii）そのような再配布のレベル値が制限値よりも少なければ、VDE管理されたコンテンツに関連するコンテンツ制御情報の１局面として、ユーザにそのようなUDEを配送する前に、再配布のレベル値を１つ増やし、再配布のレベル値が制限値と同じである場合は、そのプロセスが不履行となる）。そして、（ｂ）他の特別な制限が、再配布者に課せられることはない。

クリエーターＡによって指定される使用制御情報のいくつかは（本例においては、ユーザおよび／またはユーザ／配布者に渡される制御情報において、配布者が提供することをクリエーターが求める制御情報）、例えば、（ａ）コンテンツの移動（本明細書中で説明される配布の形態）は、許可されない、および、（ｂ）配布者は、一ヶ月の内にコンテナにアクセスしたユーザの数を計算し、かつ、レンタルが失効した後のさらなる使用を防止するために、使用パーミッション内で（少なくとも）十分な計量情報を（例えば、処理および報告のチェーン、および／または、失効日および／またはパーミッションレコードあるいは他の必要制御情報内で時間老化した（time-aged）暗号化鍵の使用によって、クリエーターＡにアクセス使用を報告するように設計された計量メソッドの使用によって）保存することを要求される。

本例で、クリエーターＡによって指定された抽出および／または埋め込み制御情報のいくつかは、コンテンツの抽出および／または埋め込みが、クリエーターＡによって提供されるVDEの保護されたコンテンツに関係する再配布権を持たないユーザを除いて、処理およびこの制御情報に関連した制御のチェーンにいるパ

ーティによって許可されないという要件を含みうる。あるいは、または、さらに、そのコンテンツの異なる部分に関して、ある抽出および／または埋め込みをイネーブルする制御情報は、本例で説明される再配布権とともに、ユーザ／配布者（ユーザ／配布者は、ユーザコンテンツアグリゲーターを含み得、ユーザコンテンツアグリゲーターは、異なるソースによって作成される、および／または、異なるソースから受け取るコンテンツを提供することによって彼ら自身のコンテンツプロダクトを作成し得る）による使用のために提供されうる。

本例の配布者Ａは、イネーブルするコンテンツ制御情報を、コンテンツアクセス権のレンタルを好むユーザおよび／またはユーザ／配布者に提供する場合に、他のアプローチよりも配布者Ａが好む基本的アプローチを選択した。本例では、クリエーターによって提供される制御情報のいくつかによって、配布者Ａがこの好ましいアプローチを直接実行することが許可され、そして、（例えば、配布者Ａがそのようなアプローチを許可し、かつ、適切な制御情報を支持する、成功したVDEネゴシエーションを完了しない限りは）他の制御構成がこの好ましいアプローチを許可し得ない。本例では、配布者Ａが受け取る制御構成の多くは、配布者Ａが、レンタルをベースとした使用権を反映する使用制御情報の作成を承認する配布制御情報に対する選択を示すVDEネゴシエーションプロセスから得られる（そして、VDEネゴシエーションプロセスの結果を反映する）。このような配布制御情報によって、ユーザおよび／またはユーザ／配布者に配布するための制御情報を作成し、結果的にアクセス権を「レンタル」するようなメソッドでクリエーターによって提供される制御構成を、配布者Ａが紹介および／または改変することが可能となる。さらに、本例における配布者Ａは、再配布権に対するユーザ／配布者からのリクエストを処理し、従って、配布者Ａによって作成された制御情報の1局面として、配布者Ａがそのような権利を包含することを許可するクリエーターとネゴシエート（または、同意）した配布制御情報もまた選択することになる。

本例では、配布者Ａとクリエーターａとが、VDEを用いて配布関係に関するネゴシエーション（例えば、VDEネゴシエーション）を行いうる。本例では、クリ

エーターＡが、VDEコンテンツコンテナと、使用権のレンタルに基づいて報酬を受け取るというクリエーターＡの望みを表す関連の制御情報とを作成し、そして、そのような制御情報が、配布者Ａがユーザ／配布者からのリクエストを処理するために使用し得る再配布制御情報に、クリエーターＡが許容可能な制限を課したことをさらに示すので、配布者Ａは、ネゴシエーションによる改変を全く行わずに、クリエーターＡの配布制御情報を受け入れうる。

クリエーターＡからのイネーブルする配布制御情報を受け取った後、配布者Ａは、アプリケーションプログラムを操作することによって、（よりシニアな制御情報によって許可される、または阻止されない場合に）配布者Ａによってイネーブルされたユーザおよび／またはユーザ／配布者のための使用制御情報の詳細のある部分または全部を指定しうる。配布者Ａは、例えば、ユーザ１人当たり１ヶ月につき１５ドルの価格が、クリエーターＡのコンテナに対するユーザの支払いに対する配布者Ａの事業目的にかなうと決定しうる。配布者Ａは、クリエーターＡによって配布者Ａに与えられた配布制御情報の要件を満たす使用制御情報を指定しなければならない。例えば、配布者Ａは、クリエーターＡの要件に応じて、制御情報の仕様書に、必要とされる失効日および／または時間老化した暗号化鍵を入れてもよい。配布者Ａが、制御情報の仕様書にそのような情報を入れなかった（または、他の要件を満たさなかった）場合には、クリエーターＡのパーミッションレコードで参照され、この制御情報を実際に作成するためにPPE650内で安全に行使される制御メソッドは、本例においては、許容可能な情報が配布者Ａの制御情報の仕様書に入れられるまでは、望ましいメソッド（例えば、あるフィールドにおける提案値のチェックに基づくメソッド、特定のメソッドがパーミッションに含まれることを求めるといった要件に基づくメソッド等）で実行されない。

本例では、ユーザＡが配布者ＡからVDEの管理されたコンテンツ使用制御情報を配布者Ａから受け取りうるように、ユーザＡが配布者Ａとのアカウントを設定しうる。ユーザＡは、配布者Ａからのコンテンツ使用制御情報を受け取ることによって、クリエーターＡのコンテンツにアクセスし、そのコンテンツを使用しう

る。使用制御情報は、配布者Ａを含む処理のチェーンを通して渡される（および、そのチェーンに加えられる、および／または、そのチェーンによって改変される）ので、クリエーターＡのコンテンツを利用するために配布者Ａからリクエストされた使用制御情報は、本例においては、クリエーターＡおよび配布者Ａからの制御情報の複合体を表す。例えば、あるユーザがクリエーターＡのVDE制御されたコンテンツコンテナにアクセスし、そのユーザが同じ月のうちにそのコンテナに以前にアクセスしていない場合に、監査レコードを生成する計量メソッドを（例えば、そのような計量メソッドのメソッドコアで参照されるオープンコンテナ事イベントに関連するUDEに、ユーザの最後のアクセス日を格納し、次のアクセス時に、そのアクセスが同じ月のうちに行われたかどうかを決定するためにその日付を比較することによって）確立しうる。１つ以上の課金、および／または、上記のような１ヶ月ごとの使用に対する料金を反映するように配布者Ａによって作成される、改変される、１つ以上のパーミッションレコードに参照される、および／または、パラメタライズされる予算メソッドを発動させる、クリエーターＡのコンテナのオープンに関連する制御メソッド（この制御メソッドは、例えば、クリエーターＡによっても作成および／または提供される、または、配布者Ａによって作成および／または提供される）において、配布者Ａは、そのような計量メソッドを利用しうる。クリエーターＡのシニア制御情報によって許可される範囲内で、配布者Ａが使用および／または再配布制御情報を指定した場合は、制御情報の新しいセット（図80に$D_A(C_A)$で示される）が、配布者Ａによるそのコンテナに関連する制御情報が、ユーザおよび／またはユーザ／配布者（本例では、ユーザＡ、ユーザＢ、およびユーザ／配布者Ａ）に配送されるときに、クリエーターＡのVDEコンテンツコンテナに関連づけられうる。

本例では、ユーザＡが、クリエーターＡのVDEコンテンツコンテナに関係する制御情報を配布者Ａから受け取りうる。この制御情報は、ユーザＡと配布者Ａとの間の拡張契約（例えば、コンテンツの使用に関連する料金、制限のある再配布権等に関する）、および、配布者Ａとクリエーターとの間の拡張契約（例えば

、ＶＤＥの制御されたコンテンツ使用情報および／または例えば配布者Ａがクリエーターから受け取る、またはクリエーターＡが配布者Ａから受け取るコンテンツ制御情報の使用および／または作成の特徴、範囲、処理、報告、および／または他の局面に関して、あるいは、他のＶＤＥのコンテンツ使用情報処理における契約）を表しうる。このような拡張契約は、各参加者のＶＤＥインストレーションの安全サブシステム内で動作する処理によって強制されうる。本例においては、配布者Ａによって改変されるような、クリエーターＡの制御情報を表すそのような拡張契約の部分は、$D_A(C_A)$によって示され、例えば、（ａ）制御構成（例えば、１つ以上のコンポーネントアセンブリ、１つ以上のパーミッションレコード等）と、（ｂ）そのような制御情報に記された要件に従って、クリエーターＡのコンテンツを使用する間に生成された使用情報の記録と、（ｃ）そのような使用の結果として（そのような結果は、ＶＤＥの使用によって配送される請求書を電子的に、安全に、かつ自動的に受け取ることも包含し得、そのような請求書は該使用から得られる）、支払い（そのような使用に応答して「実行される」自動電子クレジットおよび／または電子通貨による支払いを含む）を行うことと、（ｄ）ユーザＡ、および／または、ユーザＡのＶＤＥインストレーションのＶＤＥ安全サブシステムによる、そのような使用および／またはそのような制御情報の結果である他の活動とを含む。

制御情報$D_A(C_A)$に加えて、ユーザＡは、自分自身の制御情報を、（シニアコンテンツ制御情報の制限内で）クリエーターＡのＶＤＥコンテンツコンテナを使用する際に強制することができる。この制御情報は、例えば、（ａ）しきい値（例えば、数量制限、例えばアクティビティパラメタ当たりの出費額に対して自己的に課した制限）が超過した場合に、継続を行う前に、ユーザＡが明確な承認を与えなければならないように、使用に課した取引、セッション、時間ベースの、および／または他のしきい値、（ｂ）クリエーターＡのコンテンツに対するユーザＡの使用に関係する詳細に関係したある使用の記録および／または送信に対するユーザＡのプライバシー要件、（ｃ）クリエーターＡのコンテンツコンテナに残る価値の保存および／またはシステムの不履行または他の原因によって失い得る

電子クレジットおよび／または電子通貨の局所的格納を確実にする一助とするために、ユーザＡが自分自身に課すバックアップ要件を含みうる。ユーザＡの制御情報に関するこれらの例のうちのいくつかまたは全部における実行する権利は、ある例においては配布者とネゴシエートしうる。そのようにユーザに指定される他の制御情報は、いかなるコンテンツプロバイダから受け取るどのような制御情報とも無関係に強制され得、コンテンツおよび／または電子機器の使用の１つ以上のクラス、または全てのクラスに対する、ユーザの制御情報、より一般的には、VDEインストレーションの制御情報と関係するようにセットされうる。クリエーターＡのコンテンツコンテナをユーザＡが使用する間、適所に位置しうるVDE制御情報の完全なセットは、図80に$U_A(D_A(C_A))$として示される。このセットは、クリエーターＡによって発生した制御情報、配布者Ａによって改変されたとき、ユーザＡによってさらに改変されたときの制御情報を表し得、これらの情報はすべて、よりシニアな制御情報を提供するバリューチェーンのパーティからの制御情報に従っており、それゆえに、本例に関しては、クリエーターＡのVDEコンテンツコンテナに関する、ユーザＡと、配布者Ａと、クリエーターＡとの間の「完全な」VDE拡張契約を構成する。ユーザＢは、例えば、配布者Ａからそのような制御情報　$D_A(C_A)$も受け取り得、自分自身の制御情報を承認されたメソッドで追加することにより、セット$U_B(D_A(C_A))$を形成しうる。

ユーザ／配布者Ａは、クリエーターＡのVDEコンテンツコンテナに関係するVDE制御情報も配布者Ａから受け取りうる。ユーザ／配布者Ａは、例えば、ユーザとしてクリエーターＡのコンテンツを使用することと、制御情報の再配布者として行動することの両方を行いうる。本例では、制御情報　$D_A(C_A)$は、これら２つの活動を可能とし、かつ制限もする。$D_A(C_A)$によって許可される程度にまで、ユーザ／配布者Ａは、ユーザ／配布者Ａの使用を制御し（ユーザＡとユーザＢとに関連して上述した様式と類似の様式で）、かつ、ユーザ／配布者Ａによって再

配布される制御情報を制御する（配布者Ａと関連して上述した様式と類似の様式で）、$D_A(C_A)$に基づいた自分自身の制御情報、すなわち$UD_A(D_A(C_A))$を作成しうる。例えば、ユーザ／配布者Ａが、$UD_A(D_A(C_A))$をユーザ／配布者Ｂに再配布す

る場合、クリエーターＡまたは配布者Ａのどちらからも要求されなかった特定の使用情報を、ユーザ／配布者Ｂはユーサ／配布者Ａに報告することを要求されうる。あるいは、または、さらに、ユーザ／配布者Ｂは、例えば、ユーザ／配布者Ｂがクリエーターのコンテンツを使用する時間数（分）に基づいて（ユーザ／配布者Ｂの使用に対して配布者Ａが、ユーザ／配布者Ａに請求する月々の料金ではなく）、ユーザ／配布者Ａに、クリエーターＡのコンテンツの使用料金を支払うことに同意してもよい。

本例では、ユーザ／配布者Ａが、クリエーターＡのコンテンツに関連する制御情報をさらに再配布することをユーザ／配布者Ｂに許可する制御情報$UD_A(D_A(C_A))$を、ユーザ／配布者Ｂに配布しうる。ユーザ／配布者Ｂは、制御情報の新しいセットである$UD_B(UD_A(D_A(C_A)))$を作成しうる。制御情報$UD_A(D_A(C_A))$が、ユーザ／配布者Ｂに再配布を許可する場合、本例におけるクリエーターＡからの再配布に対する制限により、セット$UD_B(UD_A(D_A(C_A)))$がさらに再配布権を含むこと（例えば、再配布権をユーザＢに提供すること）が禁止され、その理由は、配布者Ａからユーザ／配布者Ａへの処理のチェーン（配布）と、ユーザ／配布者Ａからユーザ／配布者Ｂへのそのチェーンの継続（再配布の第１のレベル）と、別のユーザへのそのチェーンのさらなる継続とは、再配布の２つのレベルを表し、その結果、セット$UD_B(UD_A(D_A(C_A)))$は、本例においては、さらなる再配布権を包含しえない。

図79に示されるように、ユーザＢは、（数ある中で）ユーザ／配布者Ｂと配布者Ａとの両方からコンテンツを使用しうる。この例では、図80に図示されるように、ユーザＢは、クリエーターＡのコンテンツに関連する制御情報を、配布者Ａおよび／またはユーザ／配布者Ｂから受け取りうる。どちらの場合も、ユーザＢは、自分自身の制御情報を、（そのような制御情報に許可された場合）$D_A(C_A)$および／または$UD_B(UD_A(D_A(C_A)))$上にそれぞれ確立できうる。その結果それぞれ生じる制御情報のセット、$U_B(D_A(C_A))$および／または$U_B(UD_B(UD_A(D_A(C$

$_A))))$は、異なる制御シナリオを表し得、各シナリオが、ユーザＢにとって利益を有しうる。先述の例に関連して説明したように、ユーザ／配布者Ａを含む処理

のチェーンに沿って、ユーザＢがクリエーターＡのコンテンツを利用する分数に料金を基づかせる（そして、ユーザ／配布者Ａに、その月中のユーザＢによる使用量とは無関係に、ユーザ１人当たり月々15ドルの料金を配布者Ａに支払うことを要求する）制御情報を、ユーザＢはユーザ／配布者Ｂから受け取ったかもしれない。これは、配布者Ａによって提供される制御情報の直接的な使用によって要求される料金よりも、ある状況下では、より好ましいかもしれないが、再配布の使い尽くされたチェーン、そして例えば、$UD_B(UD_A(D_A(C_A)))$に含まれるさらなる使用情報報告要件という、不都合も有しうる。制御情報の２つのセット、$D_A(C_A)$と$UD_B(UD_A(D_A(C_A)))$とが許可する（例えば、あるコンテナに関係する制御情報の異なるセットの登録破棄および再登録（または、異なる制御情報を有する、および／または、異なるコンテンツプロバイダによって提供される、同一のコンテンツの複数のコピーの再登録）を、処理および$D_A(C_A)$と$UD_B(UD_A(D_A(C_A)))$に反映される制御のチェーンに対する拡張契約の１局面として、ある特定の時間の間隔内で防止する、ユーザＢのVDEインストレーションの安全なサブシステムによって使用されるオブジェクトレジストリーにおける登録間隔を例えば使って強制される排他を必要としない）場合、ユーザＢは、登録された制御情報の両方のセットを有し得、ある使用シナリオのもとで、より望ましい方のセットを利用しうる。

本例では、クリエーターＢが、VDEコンテンツコンテナを作成し、VDE制御情報のセットを、図81にC_Bとして示されるようなコンテナに関連づける。図81はさらに、クリエーターＢのVDEコンテンツコンテナに関係するイネーブルする制御情報を受け取りうるVDE参加者を示す。本例では、制御情報が以下のことを示しうる。クリエーターＢのコンテンツの配布者が、（ａ）そのような配布者に承認されたユーザおよび／またはユーザ／配布者によって復号化された情報の１キロバイトにつき0.50ドルをクリエーターＢに支払わねばならない、（ｂ）クリエーターＢが、復号化されたコンテンツの１キロバイトにつき0.50ドルを受け取る要件を維持する一方で、ユーザおよび／またはユーザ／配布者は、自分達のコンテンツコンテナを別のコンテナに埋め込むことを許可しうる、（ｃ）ユーザおよび／またはユーザ／配布者のために生成されうるイネーブルする制御情報セットの

数に制限を持たない、（ｄ）ある時間間隔で（例えば、少なくとも１ヶ月に１回）、そのような配布された制御情報の数に関する情報を報告しなければならない、（ｅ）ユーザおよび／またはユーザ／配布者が、自分達の制御情報の移動を３回まで行うことを許可する制御情報を作成しうる、（ｆ）ユーザ／配布者による制御情報の再配布を、再配布の３つのレベルまで許可しうる、（ｇ）再配布された制御情報をユーザ／配布者から受け取るユーザ１人につき１回まで移動を許可しうる。

本例では、配布者Ａが、クリエーターＢに関連して上述したVDEコンテナに関連する制御情報をユーザおよび／またはユーザ／配布者に配布することが可能な制御情報を、配布者Ａがクリエーターから要請しうる。先述のように、配布者Ａは、配布者Ａからアクセス権を受け取るユーザおよびユーザ／配布者へのアクセス権の「レンタル」をより好む事業モデルを確立した。本例におけるクリエーターＢの配布制御情報は、権利の「レンタル」を含むモデルを強制せず、むしろ、ユーザまたはユーザ／配布者によって復号化されたコンテンツの量に支払い額を基づかせる。本例では、VDEを用いることによって、クリエーターＢによって許可される異なる使用情報記録モデルを含むことを、配布者Ａがクリエーターとネゴシエートしうる。このモデルは、エンドユーザによって復号化されたバイト数を記録するクリエーターＢのコンテナに関連する制御構造において、１つ以上の計量メソッドを含むことを基調としうるが、そのような復号化に基づいて料金をユーザに請求することはしないで、むしろ、配布者Ａは、「レンタル」モデルによってユーザに請求することを提唱し、クリエーターＢの制御情報は、「レンタル」モデルによってユーザに請求できることに同意し、そして、クリエーターＢに対する支払い額を、バイト復号化計量メソッドによって記録された情報、および／または、ユーザからの支払いの集積に基づいて決定する。

クリエーターＢは、例えば、（ａ）監査人の役目を果たす（例えば、配布者Ａのサイトで VDE安全サブシステムを用いて、クリエーターＢのコンテンツのユーザから配布者Ａが受け取る監査情報の処理に関連する制御メソッドを信頼し、そ

してさらに、配布者Ａがクリエーターに返済すべき額を安全に計算すること、

そして、例えば、配布者Ａの所有するクレジットおよび／または通貨によるクリエーターＢへの支払いを管理する、互いに許容可能な予算メソッドを用いて、クリエーターＢに支払いを行う）配布者Ａとの、そのような新しい制御モデルを承諾し得、（ｂ）このコンテンツに関連するあらゆる監査機能を行う第３パーティに対する配布者Ａの承諾に基づいて、そのような新しい制御モデルを承諾し得、（ｃ）ユーザによって復号化されたバイト数を記録する１つ以上の計量メソッドに関連する情報が、配布者ＢのVDE安全サブシステムによって安全にパッケージされ、VDE通信技術を用いて、配布者Ａに加えてクリエーターＢに安全に送られた場合に、そのようなモデルを承諾し得、および／または、（ｄ）他の互いに許容可能な条件を承諾しうる。C_1によって許可されるような、配布者Ａによって行われる改変に基づいて、配布者Ａによって作成された制御情報は、本例では、$D_A(C_1)$として参照される。

ユーザＡは、制御情報のセット$D_A(C_1)$を配布者Ａから受け取りうる。配布者Ａを含む処理のチェーンを介して、クリエーターＡから受け取るコンテンツに関連して上述したように、ユーザＡは、$D_A(C_1)$に許可される範囲で、自分自身の制御情報を、制御情報$D_A(C_1)$に適用し、それによって、制御情報のセット$U_A(D_A(C_1))$を作成しうる。制御情報のセット$D_A(C_1)$は、（復号化された情報の１キロバイトにつき、0.50ドルの支払いを要求する制御情報C_1に従って、クリエーターＢのコンテンツに対するユーザＡの使用に対して、配布者Ａがクリエーターに返済すべき額の正しい計算を可能とするために）ユーザＡによって、クリエーターＢのコンテナから復号化されたコンテンツのバイト数を記録する１つ以上の計量メソッド、および、クリエーターＢのコンテンツに対するユーザＡの使用に関連し、かつ、「レンタル」モデル（例えば、配布者Ａが、ユーザＡがクリエーターＢのコンテンツを利用する月をそれぞれ記録し、そして、ユーザＡがそのようなコンテンツを利用するそのような各月ごとに、一月あたり10ドルをユーザＡに請求するさらなる制御情報に関連する、計量メソッドを例えば含み得る）に基づく課金を安全に発生させるのに十分な情報を配布者Ａが集めうるような、使用の記録に関連するさらなる計量メソッドを含みうる。

ユーザ／配布者Ａは、クリエーターＢから直接制御情報C_1を受け取りうる。この場合、クリエーターＢは、VDEを使用することによってユーザ／配布者Ａとネゴシエートし得、クリエーターＢと配布者Ａとの間に確立された配布関係に関連して上述したのと同じでありうる、または、異なりうる制御情報C_iのセットを配送しうる。例えば、ユーザ／配布者Ａは、ユーザ／配布者Ａ（および配布されたおよび／または再配布された制御情報をユーザ／配布者Ａから受け取るいかなる参加者）によって復号化されたコンテンツに対して、１キロバイトあたり0.50ドルの値段で、ユーザ／配布者Ａがクリエーターに支払うという要件を含む制御情報C_1を受け取りうる。上述のように、ユーザ／配布者Ａはまた、クリエーターＢのVDEコンテンツコンテナに関連する制御情報を、配布者Ａから受け取りうる。本例では、ユーザ／配布者Ａは、配布者Ａへと渡る処理のチェーンを通した「レンタル」料金の支払いと、クリエーターＢに向けた処理のチェーンを介した復号化の量に基づく料金の支払いとの間で選択しうる。本例では、C_1と$D_A(C_1)$のどちらか一方の使用、または、その両方の使用を選択する能力を有しうる。クリエーターＡおよび配布者Ａを含む処理のチェーンに関連して上述したように、ユーザ／配布者Ａは、C_iおよび／または$D_A(C_i)$に許可される範囲で、自分自身の制御情報を適応することによって、制御情報のセット$UD_A(C_i)$および$UD_A(D_A(C_i))$をそれぞれ形成しうる。

図81に示されるように、本例においては、ユーザＢが、クリエーターＢのVDEコンテンツコンテナに関連する制御情報を、６つの異なるソース、すなわち、クリエーターＢから直接のC_i、配布者Ａからの$D_A(C_i)$、ユーザ／配布者Ｂからの$UD_B(UD_A(D_A(C_i)))$および／または$UD_B(UD_A(C_i))$、配布者Ｃからの$D_C(C_i)$、および／または配布者Ｂからの$D_B(D_C(C_i))$から受け取りうる。これは、それを通してユーザＢが、本例における他の参加者との拡張契約に入りうる処理の６つのチェーンを表す。これらのチェーンのうち２つは、ユーザ／配布者Ｂを通過する。ユーザ／配布者ＢとユーザＢとの間のVDEネゴシエーションに基づいて、ユーザＢが、制御情報の１つまたは両方のセットを使用しうるような条件を反映する拡張契約に（両方のパーティを支配する制御情報に許可された場合）達しうる。この例では、処理および制御の２つのチェーンが、ユーザ／配布者Ｂの位置で「－

つになり」得、その後ユーザＢへと渡されうる（そして、制御情報が許可すれば、ユーザＢによる配布および／または再配布に基づいて、あとでもう一度分岐する）。

本例においては、クリエーターＣは、図82に示されるように、クリエーターＣによって作成されるVDEコンテンツコンテナに関連する、制御情報C_cの１つ以上のセットを作成する。図82はさらに、クリエーターＣのVDEコンテンツコンテナに関係するイネーブルする制御情報を受け取りうるVDE参加者を示す。そのようなコンテナ内のコンテンツは、本例においては、テキスト項目のセットに系統だてられる。本例においては、制御情報が、そのようなコンテナ内の項目を説明する１つ以上のコンポーネントアセンブリ（例えば、各項目の範囲を説明するマップテーブルおよび／またはアルゴリズムを参照する１つ以上のイベントメソッド）を含みうる。C_cはさらに、例えば以下のものを含みうる。（ａ）配布者が、ユーザおよび／またはユーザ／配布者によってアクセスされた項目１つにつき１ドルをクリエーターＣが受け取り、その支払いによって、ユーザは、そのような項目に６ヶ月間のみアクセスすることが許可されることを（例えば、１ヶ月に１度エージングするマップタイプの計量メソッド、時間老化した復号化鍵、関係のあるパーミッションレコードに関連する失効日などを用いて）確実にするという要件、（ｂ）クリエーターＣのコンテナからの項目が、抽出／埋め込み１回あたりの料金10ドルで、別のコンテナへと抽出および埋め込まれることを許可する制御情報、（ｃ）抽出された／埋め込まれた項目が、再び抽出されることを禁止する制御情報、（ｄ）配布者が、１ヶ月につき上限1000人のユーザまたはユーザ／配布者に対して、イネーブルする制御情報を作成することを許可する制御情報、（ｅ）１人の配布者によってイネーブルされるユーザおよびユーザ／配布者の数に関する情報が、少なくとも１週間に１回、クリエーターＣに報告されることを要求する制御情報、（ｆ）ユーザまたはユーザ／配布者がイネーブルする制御情報の移動を１回まで行なえるようにすることを配布者に許可する制御情報、そして、（ｇ）ユーザ／配布者による再配布を２つのレベルまで許可する制御情報。

本例では、配布者Ｂが、クリエーターＣとの配布関係を確立しうる。また、本例における配布者Ｂは、配布者Ｂに対する支払いを、そのようなVDE参加者によ

って行われるアクセス数に基づかせる制御情報をユーザおよびユーザ／配布者に配布することをより好む事業モデルを確立し得たかもしれない。本例では、配布者Ｂが、ユーザおよび／またはユーザ／配布者へ配布するイネーブルする制御情報の改変されたセット$D_1(C_c)$を作成しうる。このセット$D_1(C_c)$は、例えば、配布者Ｂから制御情報を受け取るユーザおよび／またはユーザ／配布者に対して、ユーザ１人あたり、アクセスごとに0.10ドルの料金を確立するための、VDEを用いたネゴシエーションに基づきうる。例えば、C_cに基づいて、配布者Ｂによるクリエーター Ｃへの正確な支払いを確実にするために、ユーザおよび／またはユーザ／配布者から十分な情報を集められうることを確実とするために、１つ以上のマップタイプの計量メソッドがC_cに含められた場合、そのようなメソッドは、セット$D_1(C_c)$に保存され得、そして、１つ以上のさらなる計量メソッド（および課金および／または予算メソッドのような他の必要な制御構造）が含まれ得、それによって、セット$D_1(C_c)$が、配布者Ｂが各アクセスに基づいて料金を受け取ることも確実とするように、各アクセスを記録する。

本例におけるクライアント管理者は、例えば、配布者ＢからユーザＢが受け取った管理情報とは異なるコンテンツ制御情報のセット$D_1(C_c)$を受け取りうる。例えば、クライアント管理者は、VDEを用いることによって、あらゆるクリエーター（これらのクリエーターのために配布者Ｂがイネーブルするコンテンツ制御情報をクライアント管理者に提供しうる）からのコンテンツのための制御情報のセットを確立することを、配布者Ｂとネゴシエートしうる。例えば、クライアント管理者は、クライアント管理者と配布者Ｂとの間のVDEネゴシエーションの結果を反映する制御情報のセット$D_1(C_c)$をうけとりうる。クライアント管理者は、$D_1(C_c)$に対する改変のセットを含み得、かつ、クライアント管理者と同じ組織内にいるユーザおよびユーザ／配布者（例えば、同僚、雇用人、コンサルタント等）のみに利用可能となりうる制御情報を含みうる新しいセット$C_1(D_1(C_c))$を形成しうる。そのようなアレンジメントを強制するためには、$C_1(D_1(C_c))$は、例えば、登録中に、ユーザまたはユーザ／配布者に関連するネームサービス情報を検査し、クライアント管理者に管理され、コンテンツの使用に必要とされる新しい予算メソッド等を確立する制御構造を含みうる。

配布者は、再配布権をクライアント管理者に提供し得、その再配布権によって、管理者は、あるコンテンツのためのパーミッションレコードを作成する権利（そのコンテンツを使用するための再配布権）を、管理者の組織内においてのみ再配布でき、そして他のパーティには再配布がおこなえない。同様に、そのような管理者は、そのような「制限された」権利を拡張することにより、自分の組織内の部署および／または他の管理者に再配布でき、そのような権利を再配布することにより、個人および／またはクラスおよび／または管理者によって規定されるような組織人事の他の分類の１つ以上の制限されたリストに基づいてコンテンツを使用しうる。再配布をある１つ以上のパーティおよび／またはクラスおよび／またはVDEユーザの他の分類および／またはインストレーションに限定するこのVDEの能力は、そのような制御がシニア制御情報によって許可される限り、どのようなVDEコンテンツプロバイダによっても、コンテンツに適応することができる。

本例におけるユーザＤは、クライアント管理者とユーザ／配布者Ｃのどちらか一方から、または両方から制御情報を受け取りうる。ユーザ／配布者Ｃは、例えば、ユーザＤのアクションに対して、追加的なレベルの制御を維持することをユーザ／配布者Ｃに許可する、ユーザ／配布者Ｃによって管理される各部門ごとの予算メソッドを含む制御情報$UD_c(C_A(D_B(C_c)))$を、ユーザＤに配布しうる。本例では、$UD_c(C_A(D_B(C_c)))$は、商用の配布チャンネルから生じる制御に加え、複数のレベルの組織的制御（例えば、クライアント管理者に起源を持つ制御およびユーザ／配布者Ｃに起源を持つさらなる制御）を含みうる。さらに、または、あるいは、クライアント管理者が、ポリシー、プロシージャ、および／または他の管理プロセスに従って、クライアント管理者の組織を通って流れる制御情報を確実にする一助となる十分な制御情報（例えば、ユーザＤなどのユーザへの再配布を許可する、ユーザ／配布者Ｃに配布された制御情報）を有していたとしても、クライアント管理者が、あるクラスの制御情報を、ユーザＤに配布することを拒絶しうる。

本例では、ユーザＥが、クライアント管理者および／または配布者Ｂから制御情報を受け取りうる。例えば、ある制御情報がクライアント管理者から受け取ら

れ得たとしても、ユーザEは、配布者Bとのアカウントを有しうる。この場合、

ユーザEは、制限なしに、配布者Bから制御情報を要請および受け取ることを許可されうる、または、組織的ポリシーとして、クライアント管理者は、ユーザEと配布者Bとのインタラクションの範囲を制限するユーザEの電子機器に関連する場所に制御情報を有してもよい。後者の場合、クライアント管理者は、ユーザEが、クライアント管理者からは利用不可能で、1つ以上の特定のクラスの配布者および／またはクリエーターからは利用可能で、および／または一定のプライスポイント（例えば1時間の使用につき50ドル）などの使用に対するコストを有するユーザEの電子機器の安全サブシステムに制御情報を登録することを制限しうる。あるいは、または、さらに、クライアント管理者は、例えば、ユーザEが、クライアント管理者からの制御情報において利用可能な価格（または、他の基準）よりも好ましい価格（または他の制御情報基準）を受け取るような制御情報を、ユーザEが配布者Bから受け取ることを制限しうる。

本例では、クリエーターDが、他のコンテンツ、例えば、クリエーターBおよびクリエーターCに提供されたコンテンツと一体化するように主に設計されたVDEコンテンツコンテナを、（例えば、VDE抽出／埋め込みプロセスの使用によって）作成しうる。図83は、クリエーターDによって作成されたVDEコンテンツコンテナに関係するイネーブルする制御情報を受け取りうるVDE参加者を示す。クリエーターDのコンテンツに関連する制御情報（図83におけるC_0）は、例えば以下のものを含みうる。（a）1回のオープンにつきユーザ1人あたり1.50ドルまたはユーザ1人あたり無制限のオープンに対して25ドルのどちらかの支払いを配布者が行うという要件、（b）クリエーターDによって作成された他のあるコンテンツに対する無制限のオープンに対して予め支払いをすませたユーザに対する20％の割引（例えば、そのような他のコンテナのいずれかが登録されたかどうかを決定する、そしてさらに、このコンテナに対する権利を購入するユーザが所有する権利の特徴を決定するために、ユーザのVDEインストレーションの安全データベースを分析する1つ以上の課金メソッドを含むことで実行される）、（c）配布者が、C_0に従って作成された制御情報によってイネーブルされたユーザお

よびユーザ／配布者の数を、1000人を超えた後に報告するという要件、（ｄ）配布者が、ユーザおよび／またはユーザ／配布者による移動の数を１回の

みに限定するという要件、（ｅ）配布者が、ユーザ／配布者に、再配布のレベルが４を超えないように限定する要件、および、（ｆ）配布者は、他の配布者が制御情報を配布者として作成することを許可するイネーブルする制御情報を作成しうるが、配布者は、そのようなイネーブルされた配布者にこの能力を渡し得ず、そして、そのようにイネーブルされた配布者による制御情報の使用に関連する監査情報が、処理を行うことなしに、そのようなイネーブルする配布者によって直接クリエーターＤに渡され、かつ、クリエーターＤが、そのようなイネーブルする配布者に、そのようなイネーブルされた配布者からクリエーターＤが受け取る支払いの10％を支払うことをさらに要求する、イネーブリング制御情報を配布者が作成しうるという要件。

本例では、配布者Ｃが、クリエーターＢ，クリエーターＣ，および、クリエーターＤからのVDEコンテンツコンテナと、関連の制御情報のセットＣ$_{B}$、Ｃ$_{C}$およびＣ$_{D}$とを受け取りうる。配布者Ｃは、埋め込み制御情報および他の制御情報を利用することによって、クリエーターＢ、クリエーターＣ，およびクリエーターＤから受け取った２つ以上のVDEオブジェクトを有する新しいコンテナを作成しうる。さらに、または、あるいは、配布者Ｃは、そのような受け取られたコンテナのそれぞれに対して、ユーザおよび／またはユーザ／配布者（Ｃ$_{D}$の場合は配布者）に配布されるイネーブルする制御情報を作成しうる。例えば、配布者Ｃは、クリエーターＢ，クリエーターＣ，およびクリエーターＤからのコンテンツ部分を含むコンテナ（例えば、埋め込まれたコンテナ）を作成し得、そのコンテナ内では、そのような部分のそれぞれが、配布者Ｃによってイネーブルされたユーザおよび／またはユーザ／配布者に関係する使用アクティビティに基づいて、そのようなクリエーターがそれぞれ、配布者Ｃからの支払いを安全かつ確実に受け取るための十分な情報を記録し、かつ、監査人がその十分な情報を集めることを許可する、アクセスおよび使用に関係する制御情報を有しうる。さらに、配布者Ｃは、VDEを用いてそのようなクリエーターのうちの数人または全員とネゴシエ

ートすることによって、C_1、C_2および／またはC_3に基づいた、配布者Ｃによるそのようなクリエーターへの支払いに関する、そして例えば、コンテンツの使用情報および関連の（例えば、公告）情報の集合に対する異なるモデルのそれぞれから生じた、そのようなクリエーターそれぞれのモデルを維持する一方で、配布者Ｃが、ユーザおよび／またはユーザ／配布者に請求される「一定の」料金（例えば、１ヶ月ごと、または、アクセスごとに合同モデルから計算される等）に基づいて、コンテナ全体に対する総合的な制御情報を提供するモデルをイネーブルしうる。

本例では、配布者Ｂは、図83に示されるように、クリエーターＥから、VDEコンテンツコンテナおよび関連のコンテンツ制御情報C_1を受け取りうる。C_1が許可するなら、配布者Ｂは、そのようなコンテナのコンテンツの１部分を抽出しうる。配布者Ｂは、その後、例えば、クリエーターＢ、クリエーターＣ、およびクリエーターＤによって作成されたVDEオブジェクトの集合を含む、配布者Ｃから受け取ったコンテナにこの部分を埋め込みうる。各クリエーターおよび配布者Ｃから受け取った制御情報のセットにおける特定の制限および／またはパーミッションに応じて、配布者Ｂは、例えば、そのような抽出された部分を、配布者Ｃから受け取ったコンテナに、独立したVDEオブジェクトとして埋め込むこと、または、クリエーターＢ、クリエーターＣ，および／またはクリエーターＤからの「適所にある」オブジェクトのコンテンツに直接埋め込むことができうる。あるいは、または、さらに、配布者Ｂは、もしC_1が許可するなら、そのような抽出されたコンテンツの部分を、独立したVDEオブジェクトとして配布することを選択しうる。

本例では、ユーザＢは、クリエーターＢ、クリエーターＣおよびクリエーターＤによって作成されたVDEオブジェクトから成るVDEコンテンツコンテナを、配布者Ｃから受け取りうる。さらに、ユーザＢは、クリエーターＥによって作成されたコンテンツの１つ以上の抽出された／埋め込まれた部分に加えて、クリエーターＢ、クリエーターＣ，およびクリエーターＤによって作成された同一のコンテンツを含むVDEコンテンツコンテナを、配布者Ｂから受け取りうる。ユーザＢは

、そのようなコンテナのうちどれを使用するかの選択（埋め込まれたコンテナのどれを使用したいかを含む）に関する決定を、例えば、そのような抽出された／埋め込まれた部分の特徴（例えば、コンテンツの残りの部分において可能性のある興味分野を示すマルチメディアプレゼンテーション、解説的に説明するおよび／

または解説するコンテンツの他のエレメント、関連の仕事、コンテンツのエレメントとして配送される向上したアプリケーションソフトウェアなど）；そのような部分の品質、有用性、および／または価格（あるいは制御情報の他のアトリビュート）；コンテナ、および／または、本例においては配布者Ｂおよび配布者Ｃから受け取ったコンテンツ制御情報を区別する他の要件に基づかせうる。

ユーザＢは、ユーザがその中に含まれるコンテンツを追加および／または改変することを許可するそのようなVDEコンテンツコンテナのためのコンテンツ制御情報を、配布者Ｂから受け取りうる。ユーザＢは、例えば、VDEを意識しているワードプロセッサまたは他のアプリケーションを使用するようなコンテナにおいて、コンテンツに注釈をつける能力を要望しうる。シニア制御情報に許可されるならば、コンテンツのある部分または全部が、改変および／または追加を行うために、ユーザＢに使用可能となりうる。この場合、ユーザＢは、追加されたおよび／または改変されたコンテンツのVDEクリエーターとしての役目をはたしている。ユーザＢは、例えば、そのようなコンテンツに対する新しい制御情報を提供しうる、または、そのようなコンテンツを（そのようなコンテナおよび／または含有されたオブジェクトに関係する制御情報に基づいて）管理するために、現存する制御情報（または、この目的のために、処理のチェーンにおけるシニアメンバーによって含まれる制御情報）を利用することを要求されうる（または望まれうる）。

本例では、VDE100は、例えば、コンテンツの配布、再配布、アグリゲーション（抽出および／または埋め込み）、リアグリゲーション、改変、および使用を含む環境をイネーブルするために使用された。本例における環境によって、制御情報とコンテンツの両方がネゴシエートされ得、かつ、それを通して制御情報およ

び／またはコンテンツが渡された処理のチェーンに基づいた異なる事項を有しうる競争的なモデルが可能となる。さらに、本例における環境によって、そのような活動をイネーブルする制御情報を受け取るVDE参加者にコンテンツを追加すること、および／または、そのようなVDE参加者によってコンテンツが改変されることが許可される。

例－コンテンツVDEチェーン処理を通したコンテンツ配布

図８４は、VDE参加者の幾つかのカテゴリーを含む、VDEコンテンツ配布の比較的簡単なモデル3400の特定の局面を表している。この事例において、リファレンス目的の簡略化のために、コンテンツの多様な部分がVDEコンテンツコンテナオブジェクトの形式で、別個のアイテムとして表されている。そのような１以上のコンテンツ部は、単一オブジェクトに一体化され得、また（コンテンツ制御情報によって許可されるなら、いずれのVDEコンテンツコンテナのコンテンツでもあり得る）ユーザによって全体もしくは部分で抽出され得る。この例において、歴史／教育マルチメディアコンテンツの発行者は、３つのコンテンツ資源から利用可能なコンテンツオブジェクトを使用することにより、VDEコンテンツコンテナを作成している。

・発行者に利用可能な、光ディスク上のビデオライブラリ3402プロダクトであり、多様な歴史的場面を表すビデオクリップVDEオブジェクトを含む。

・歴史情報テキストおよび画像資源をVDEオブジェクトに格納するインターネット容器3404であり、VDEオブジェクトは発行者および他のユーザにダウンロードできる。

・光ディスク上で利用可能なオーディオライブラリ3406であり、単独もしくは他の教育的、歴史的材料と共に使用することができる多様な演奏および音声（例えば、歴史ナレーション）ピースを含む。

ライブラリ3402、容器3404、およびライブラリ3406に提供された情報は、異なる発行者3408(a)、3408(b)～3408(n)に提供され得る。その後発行者3408は、得た情報の一部もしくは全部をユーザ3410に提供する。

この例において、ビデオライブラリ3402制御情報は、発行者がビデオライブラ

リプロダクトコンテナからオブジェクトを抽出することを許可し、オブジェクトが50ドルより少ないライセンスコストであり、および持続時間が45分より短く、および抽出した他のオブジェクトのいずれもがそれぞれ20,000コピーであり、さらに全てのビデオオブジェクトに複号上へのVDE指紋刻印を要求する場合、各抽出したオブジェクトを１年間使用可能にするコンテンツ制御情報を抽出することを許可する。オーディオライブラリ3406は、ビジネスモデルに合致する、同様の制御を確立している。インターネット容器3404VDEは、オブジェクトのダウンロードというユーザの要求であるオンラインに応答して、選択されたオブジェクトコンテンツが容器から流れ出す時に、選択されたオブジェクトコンテンツを、暗号を含めてコンテナライズする。容器3406は、暗号化および発行者への通信に先だって、コンテンツ内に、受け取るVDEインストレーションの識別を指紋刻印し得る、および発行者もしくは他のコンテンツユーザによって複号化される際に、コンテンツのユーザ識別指紋刻印をさらに要求し得る。

提供資源とネゴシエートした（もしくは同意した）条件および状況下で、この例における発行者3408は、顧客の教師のためのVDEオブジェクトコンテナプロダクトを形成するために複合させる、多様なコンテンツピースを選択する。発行者3408(A)は、ビデオライブラリ3402から抽出されたビデオオブジェクト（円で表されている）、インターネット容器3404から抽出されたテキストおよびイメージオブジェクト（ダイアモンドで表されている）、およびオーディオライブラリ3406から抽出された１つの演奏曲および歴史ナレーション（長方形で表される）を複合する。発行者3408(B)は、発行者3408(B)のプロダクトに複合する、同様の配列のオブジェクトを抽出し、プロダクトをさらにエンハンスするために、発行者3408(B)によって作成されたグラフィックエレメント（六角形であらわされる）をさらに加える。発行者3408(C)はまた、インターネット容器3404およびオーディオライブラリ3406から抽出されたオブジェクトを複合することによって、プロダクトを作成する。この例において、組み込んだオブジェクトを伴うVDEコンテンツコンテナオブジェクトの形式の、それぞれの光ディスク上の全ての発行者プロダクトは、高校のコンピュータネットワークにインストールするために、現代

の高校に配送される。

この特定の例においてエンドユーザ3410は教師であり、発行者のプロダクトをサポートする、教師の高校のサーバ上のVDEインストレーションにアクセスするために、教師のVDEノードの安全サブシステムを使用する（代替例において、高校はサーバベースのVDEインストレーションのみを維持する）。教師は、１以上の発行者からのVDEプロダクトをライセンスし、VDEプロダクトコンテンツコンテナから所望のオブジェクトを抽出、およびもしくは抽出したVDEコンテンツをVDEコンテンツコンテナの形式で、教師の教室のコンピュータに適度に、および／もしくは効率的に格納するために、ダウンロードする。教師は抽出されたコンテンツをVDEコンテンツコンテナの形式で、サーバマスストレージ上に格納し得る（および／もしくは、もしエンドユーザにとって望ましく役に立つのならば、およびさらには容認できるプライシングおよび／もしくは他の条件および状況および／もしくはシニアコンテンツ制御情報に従うならば、教師は、教師のノードおよび／もしくはサーバ格納手段に、抽出した情報を「クリア」な暗号化されていない形式で格納し得る）。このことにより、教師は、発行者のプロダクトの選択された部分をプレイおよび/もしくは使用することができ、およびこの例の２つの事例に示されるように、教師はオブジェクトに、コンテンツを作成した教師および/もしくは生徒をさらに加えることができる。エンドユーザ3410(2)は、例えば、発行者Ａから受け取ったビデオピース１を選択しており、発行者Ａはビデオライブラリからそのオブジェクトを受け取っている。ピースは発行者3408(B)からも利用できるが、おそらくは好ましい条件および状況下（サポートコンサルテーションテレホンラインなど）にないため、エンドユーザ3410(3)も同じ発行者3408(A)からビデオピース３を受け取っている。加えて、エンドユーザ3410(3)は、歴史リファレンスピース７のコンテンツに対応するオーディオ歴史ナレーションを、発行者3408(B)から受け取る。エンドユーザ3410(3)はまた、発行者3408(2)から、対応する歴史リファレンスピース７（本）を受け取っており、発行者3408(2)はその本をインターネット容器3404から受け取っている。この事例において、エンドユーサ3410(3)は、同じ本をキャリーする発行者3408(1)ではなく、発行

者3408(2)から歴史リファレンスピース７をライセンスしているため、おそらく少なめの料金をその本に対して課される。エンドユーザ3410(3)は、教師として、彼女が彼女のクラスに最も適当と思うアイテムを選択し、VDEの使用を通じて、そのようなアイテムを、彼女に利用可能な資源から意のままに抽出することが可能となっている（この場合、発行者によって提供される、および地元高校ネットワークサーバ上で利用可能な多様な光プロダクトからオブジェクトを抽出すること）

例--組織内でのコンテンツ制御情報の配布

図８５は、２つのVDEコンテンツコンテナである、コンテナ300(A)およびコンテナ300(B)を表し、それらは大きな組織におけるVDEクライアント管理者3450に配布されている。図に示すように、コンテナ300(A)およびコンテナ300(B)は、会社に到着する際に、組織が利用可能な使用権を指定する、特定の制御情報を運んでいる。さらに図８５に示すように、クライアント管理者3450は、セールスおよびマーケティング管理者3452(1)、プランニング管理者3452(2)、および調査開発管理者3452(k)などの、組織の特定の部門管理者3452にこれらの権利の特定のサブセットを分散させる。各場合において、クライアント管理者3450は、各部門にどの使用オプションが利用させるか、および予算はいくらかを決定する。

図８５は簡略化された例であり、例えば、クライアント管理者3450は、クライアント管理者3450によって作成されたVDE制御をさらに加え得る、および／もしくは位置制御において改変および／もしくは削除し得る（制御情報によって許可された場合）、および／もしくはさらには利用可能な財政予算（または他の予算）を特定の使用活動の間で分割し得る。この例において、部門別管理者は、クライアント管理者が部門に関して有するような、部門別エンドユーザの権利を決定するための、同一の権利を有している。加えて、この例において（しかし、図８５には図示せず）、クライアント管理者3450および／もしくはコンテンツプロバイダはまた、エンドユーザコンテンツ使用および／もしくはエンドユーザの全てまたは特定のクラスの使用の結果を直接的に制御する（関連する配布権利を含む）、特定の制御情報を決定し得る。図８５に示す例において、組織内にはたった

３つのレベルのVDE参加者しかいない。

クライアント管理者3450

部門管理者3452、および

エンドユーザ3454

である。

他の例において、VDEは組織（例えば、部局、部門、プロジェクト、ネットワーク、グループ、エンドユーザ等）内の多くのレベルのVDE管理（重複するグループを含む）をサポートする。加えて、VDEモデルにおける管理者は、それ自体もまたVDEコンテンツユーザであり得る。

組織内において、VDEインストレーションは、各エンドユーザ3454ノードにおいて行われ得、サーバのみもしくは他の複合的なユーザコンピュータ、もしくは他の電子器具、もしくは混合環境であり得る。VDEサーバおよび／もしくはノード使用の混合に関する決定は、組織および／もしくはコンテンツプロバイダセキュリティ、性能、間接費、もしくは他の理由に基づき得る。

この例において、図８５におけるVDE参加者間の通信には、VDE安全通信技術を、PPEをサポートするVDE安全サブシステム間に用いており、また他のVDE安全システム構成要素を、組織内における各VDEインストレーションに用いている。

例--他のコンテンツ配布例

VDE保護化コンテンツのクリエータは、多くの異なる方法で他のVDE参加者と対話し得る。VDEクリエータ102は、例えば、コンテンツおよび／もしくはコンテンツ制御情報を直接的にユーザに配布し得、コンテンツおよび／もしくはコンテンツ制御情報を商業コンテンツ容器に配布し得、コンテンツおよび／もしくはコンテンツ制御情報を会社コンテンツ容器に配布し得、および／もしくはコンテンツおよび／もしくはコンテンツ制御情報を他のVDE参加者に配布し得る。クリエータ102が、クリエータのコンテンツの全てのユーザと直接的に対話しない場合、クリエータは、VDE参加者がコンテンツおよび／もしくはコンテンツ制御情報をさらに配布することを許可する配布パーミッションを、他のVDE参加者に伝送し得る。クリエータはまた、例えば、制御情報の再配布を制限しないことによって

、もしくは他のパーティに受け渡すことのできる１以上のパーミッション記録のための「コンジット」としてVDE参加者が働くことを許可することによって、VDEコンテンツおよび／もしくはコンテンツ制御情報のさらなる配布を許可し得、そのパーミッション記録は、第１の受け取りパーティおよび／もしくは第２の受け取りパーティの識別を含むことを認める。

図８６は、VDE参加者の可能な配置を示している。この例において、クリエータ102は、VDE保護化形式（例えば、１以上のVDEコンテンツコンテナ内に）内に非暗号化されたコンテンツを配置するために、１以上のアプリケーションソフトウェアプログラムおよび１以上のVDE安全サブシステムを用い得る。加えて、クリエータ102は１以上の配布パーミッション3502および／もしくは使用パーミッション3500を、そのようなVDE保護化コンテンツと関係する制御情報の局面として生成し得る。そのような配布および／もしくは使用パーミッション3500、3502は同一であり得（例えば、全ての配布パーミッションは実質的に、全く同一の特徴を有し得る）、もしくはそれらが生成された対象である参加者のカテゴリーおよび／もしくはクラス、それらが要求および／または伝送される際の環境、クリエータ102もしくは受け手等いずれかのコンテンツ制御モデルの変化などに基づいて異なり得る。

この例において、クリエータ102は、VDE保護化コンテンツをユーザ112a、ユーザ112b、および／もしくはユーザ112cに伝送する（例えば、ネットワーク上で、放送を介して、および／もしくは物理的媒体のトランスファーを通じて）。加えて、クリエータ102はVDE安全通信技術を用いて、そのようなユーザに使用パーミッションを伝送する。ユーザ112a、ユーザ112b、およびユーザ112cは、クリエータ102から受け取った使用パーミッションによって指定された制御情報の制限内で、そのようなVDE保護化コンテンツを用い得る。このケースにおいて、クリエータ102は例えば、クリエータ102によってユーザに伝送されたVDE保護化コンテンツに関連する、そのようなユーザ活動の全ての局面を管理し得る。あるいは、クリエータ102は例えば、ユーザに利用可能でなくてはならない、クリエータによって提供されない（例えば、他のパーティによって管理される構成要素アセン

プリ）情報を制御するために、リファレンスを含み得る。

商業コンテンツ容器200gは、この例において、VDE保護化（もしくは、異なった方法で、安全に配送された）コンテンツおよび配布、パーミッションおよび／もしくは他のコンテンツ使用制御情報を、クリエータ102から受け取り得る。商業コンテンツ容器200gはコンテンツを安全に格納し得るために、いずれの必要とされるコンディションが揃った際、ユーザはそのようなコンテンツを容器200gから手に入れ得る。配布パーミッション3502は、例えば、商業コンテンツ容器200gが、クリエータ102から受け取ったコンテンツ制御情報に記載される、特定の制限をうけたVDE保護化サブシステムを用いて、再配布パーミッションおよび／もしくは使用パーミッション3500、3502を生成することを可能にし得る（例えば、特定の枚数のコピーを超過しないこと、商業コンテンツ容器200gによる、クリエータ102への特定の支払いを要求すること、そのようなパーミッションの受け手に、コンテンツ使用情報等に関する特定の報告要求に合致するように要求すること）。そのようなコンテンツ制御情報は容器インストレーションに格納され得、またユーザの要求に応答してその容器から伝送される際に、非暗号化されたコンテンツに適用され得、そのコンテンツは、そのようなコンテンツをユーザに通信する安全なプロセスにおけるステップとしてVDEコンテナ内に配置される。再配布パーミッションは、例えば、そのようなパーミッションの受け手が、特定の制限（例えば、同一の家族、他のビジネス組織のメンバーに限る等）を受けた、特定の数の使用パーミッションを生成することを許可し得る。容器200gは、例えば、クリエータ102から受けとった制御情報によって、容器がパーミッションを配布した対象であるすべてのVDE参加者からのコンテンツ使用情報を、集めて報告することが要求され得る。

この例において、パワーユーザ112dは、デスクトップコンピュータ3504を用いて、商業コンテンツ容器200gからVDE保護化コンテンツおよび再配布パーミッションを受け取り得る。パワーユーザ112dはその後、例えば、デスクトップコンピュータ3504、ラップトップコンピュータ3506、および／もしくはセットトップ器具3508のための使用パーミッションを生成するために、そのようなデスクトップ

コンピュータ3504のVDE安全サブシステムとの接続にアプリケーションソフトウェアを用い得る（商業コンテンツ容器200gから受け取った再配布パーミッションが、そのような活動を許可すると仮定して）。シニア制御情報（例えば、クリエータ102から。容器200gによって改変されている）によって許可される場合、パワーユーザ112dは、そのような使用パーミッションに独自の制限を加え得る（例えば、ユーザ識別情報に基づいて、パワーユーザ112dの家族の特定のメンバーのセットトップ器具の使用を、１日あたり特定の回数、使用量等に制限する）パワーユーザ112dは、その後そのようなVDE保護化コンテンツおよび使用パーミッションを、VDE安全通信技術を用いて、ラップトップコンピュータ3506およびセットトップ器具3508に伝送し得る。このケースにおいて、パワーユーザ112dは、デスクトップコンピュータ3504からセットトップ器具3508およびラップトップコンピュータ3506にパーミッションを再配布し、セットトップ器具およびラップトップコンピュータは、デスクトップコンピュータに定期的にコンテンツ使用情報を報告することを要求され得る。その後、デスクトップコンピュータはユーザ使用情報を収集し、および／もしくは処理し、および容器200gにユーザ使用情報を報告し得る。

ユーザ112eおよび／もしくは112fは、商業コンテンツ容器200gから使用パーミッションおよびVDE保護化コンテンツを受け取り得る。このようなユーザは、そのような使用情報によって承認された方法で、そのようなコンテンツを用いることができ得る。パワーユーザ112dとは対照に、これらのユーザは、容器200gから再配布パーミッションを要求され得ないおよび／もしくは受け取り得ない。このケースにおいて、そのようなトランスファーおよび／もしくはが、容器200gから受け取った使用パーミッションによって許可される場合、これらのユーザは、幾つかもしくは全ての使用パーミッションを他の電子器具600にトランスファーすることができ得、および／もしくはユーザは権利の幾らかを他の電子器具に移行させることができ得る。このケースにおいて、そのような他の器具は、容器200gに直接的に使用情報を報告することができ得る。

この例において、会社700内における会社コンテンツ容器702は、VDE保護化コ

ンテンツおよび配布パーミッションをクリエータ102から受け取り得る。会社容器702によって受け取られた配布パーミッションは、例えば、容器702の配布活動を会社700内に限定する制限を含み得る。

容器702は、例えば、VDE保護化コンテンツ、および／もしくは再配布および／もしくは使用パーミッションを受け取るおよび／もしくは伝送するために、VDE安全サブシステムに連結して作動する、自動化されたシステムを用い得る。このケースにおいて、自動化されたシステムは、例えば、パーミッションの特徴および／もしくは会社700内の多様なパーティ（会社グループおよび／もしくは個人）に配送されたコンテンツを決定するために、会社の方針、部門別の方針、およびユーザの好みによって規定される標準に頼り得る。そのようなシステムは、例えば、クリエータ102から配布パーミッションを受け取る会社700に応答して、

自動的に部門別コンテンツ容器704に対して再配布パーミッションを生成し得る、および／もしくはユーザ112jおよび／もしくはユーザ112kに対して使用パーミッションを生成し得る。

部門別容器704は、ユーザ112g、ユーザ112h、および／もしくはユーザ112iに対して自動的に使用パーミッションを生成し得る。そのようなユーザは、部門別容器704から使用パーミッションを受け取るにも関わらず、会社コンテンツ容器702からコンテンツをアクセスし得る。このケースにおいて、ユーザ112g、ユーザ112h、および／もしくはユーザ112iは、シニア制御情報によって強いられる制限に加えて、部門別制限を含む部門別容器704から、使用パーミッションを受け取り得る（この例において、例えばクリエータ102から。会社容器702によって改変されている場合、部門別容器704によってさらに改変されている場合があり、会社および／もしくは部門別の方針および会社700の会社の人事への同意に加えた、クリエータ102および会社700の商業的要求を含む、VDE拡張化同意を反映する）

例―「仮想シリコンコンテナ」

上述したように、ある例におけるVDEは、「仮想シリコンコンテナ」（仮想ブラックボックス）を提供し、SPU500の幾つかの異なる事例は、複合的な位置およ

び電子器具600に「仮想に」存在する総合安全ハードウェア環境を提供するために、共に安全に通信し得る。図87は、仮想シリコンコンテナのモデル3600を表す。この仮想コンテナモデル3600は、コンテンツクリエータ102、コンテンツ配布者106、1以上のコンテンツ再配布者106a、1以上のクライアント管理者700、1以上のクライアントユーザ3602、および1以上の手形交換所116を含む。これらの多様なVDE参加者のそれぞれは、少なくとも一部、シリコン基板半導体ハードウェア素子安全処理ユニット500を包含し得る保護された処理環境655を含む電子器具600を有する。多様なSPU500は、仮想配布環境の一部をそれぞれカプセル化し、その後一緒に仮想シリコンコンテナ3600を形成する。

例--テスト実施／試験

高校最上級生のための、予定されたSAT試験は、Educational Testing Service によって準備される。発表予定の1994年11月15日の東部標準時1:00PMまで、試験はVDEコンテナ内に配置される。SATは、各学校もしくは試験を行う他の場所のために、コンテナのコピーを1つづつ用意する。学校もしくは他の場所（テスト予定地）は、配布された、テスト予定地の「管理」電子器具および／もしくはテスト管理者（テスト組織など）および、例えば200のテストVDEコンテンツコンテナの生成を可能とする予算のためのVDE識別を安全に含んでいる試験コンテナを備えることになる。テスト予定地で生成された各コンテナは、各電子器具600のための安全識別情報を含むパーミッション記録をテスト予定地のネットワーク上に有し得、例えばテストを受ける生徒のための識別と同様に、テスト受験者によって用いられる。生徒の識別は、例えば、テストを受けるに先だって生徒によって入力される安全PINパスワードの形式であり得る（テストモニタもしくは管理者は、PINパスワードを入力することによって生徒の識別を検証し得る）。当然、識別は、自動音声認識、筆跡認識（署名認識）、指紋情報、目視認識、もしくは同様の1以上の認識形式をとり得、それらはテスト受験者（および／もしくはテストモニタ／管理者）のIDを確認するために用いられ得る、および／もしくはVDEコンテナ等に、または特定のコンテナ情報によって指された場所に、テスト結果と共に格納し得る。この識別は、暗号化されたもしくは非暗号化された形式で

格納され得る。暗号化された形式もしくは他の保護形式で格納された場合、エラー修正情報などの特定の概要情報は、識別に対応するとして、関連したテストを認証するために、識別情報と共に格納され得る。

生徒がコンピュータ端末を用いてテストを受けるにつれて、選択された解答は速やかに、安全に格納され得る（しかし、解答は生徒によってテスト時間中に変更され得る）。テストが完了すると、テストのリファレンスに沿って、生徒の解答はVDE報告オブジェクトに安全に格納され、VDE報告オブジェクトはネットワークに沿って、テスト管理者および管理電子器具600に受け渡される。全ての生徒のための全てのテストオブジェクトは、その後、Educational Testing Serviceへの通信のために、平均および平均得点を示す概要情報、および要約するために望ましい情報、および／もしくは送られたテストオブジェクトの認証として働き得る情報を含む他の関連情報（VDE100によって安全にされてもよい）と一緒に、

VDEオブジェクト300内に配置でき得る。例えば、「真正の」テストオブジェクトとしてのオブジェクトの有効性を検査するものを助ける情報を含む、各生徒の概要オブジェクトから、特定の情報が別々に送られ得る。

VDEをテスト実施シナリオに適用することは、テスト実施に先だってテストにアクセスすることから生じるカンニングを、大幅に排除し得る（普通、テストは教師もしくはテスト管理者から盗まれる）。ETSにおいて、テストへのアクセスを有する個人は、テスト「全体」の盗難のリスクを排除するために、（そのアクセスは）テストの一部に限定され得る。完全に真正のテスト結果は、妥当な期間保管出来るため、VDEを用いることことにより、処理エラーもしくはテスト解答の他の操作が防ぎ得る。

全体としては、VDE100を電子テスト実施のために用いることは、電子格納、電子通信、およびテスト材料およびテスト実施結果の電子処理に関連する実質的リスクなしで、電子テスト実施の利点を提供することを可能にする。電子テスト実施は効率を大きく改善し、印刷、積出し、出荷、およびテストの人間による処理を排除することによって、テストの実施および処理のコストを著しく低下させる。同時に、電子テスト実施は、テスト期間が過ぎた際にユーザがテスト結果のコ

ピー（暗号化された、もしくは非暗号化された）を受け取ることを可能にする。これは、テストを受けた個人がテスト結果を紛失する、もしくはテスト結果が不適当に処理されることを防ぐ。VDE100を用いた電子テスト実施はまた、テスト実施のタイミング関連変数（例えば、正確な開始、持続時間、および停止時間）を信頼性高く管理でき得ることを可能にし得る。当然、テスト実施処理にVDE100を適切に使用することは、テスト実施に先だった、テストコンテンツへの不適切なアクセスを防ぐことができ、また誰がどのテストを受け、いつ、どの電子器具で、どの予定地でテストを受けるかというテスト受験が、適切に監査および認証されることを確実にする。紛失、盗難、不適切な時間合わせ、もしくは他の変数による再テスト実施は、避けられるもしくは排除することができる。

VDEを補助したテスト実施は、当然、安全／認証目的のため、雇用（例えば仕事申し込み）申し込みのため、および全ての範囲の評価テスト実施のためを含む多くの異なる応用のために用いられ得る。例えば、航空路のパイロット、もしくはトラック、電車、もしくはバス運転手は、疲労、薬物使用等に対する警告度を評価するテストと共に、出発に先だってもしくは旅行の最中に速やかにテストを受け得る。特定のテストは、テストを受ける度にもしくはグループ毎に、異なる順序および／もしくは組合せのテスト活動を有し得る。テストもしくはマスターテストは、VDEコンテナに格納され得る（テスト問題の順序、およびどの問題かは、PPE650で安全に実行された処理によって決定され得る）。テスト応答はそれらが生じた際に暗号化され得、またアグリゲートされた（もしくは他のテスト結果）伝送のために局部的に格納され得る、もしくは動的に伝送され得る（例えば、中央テスト管理コンピュータへ）。テスト受験者がテストを「失敗した」場合、おそらく彼もしくは彼女は、乗り物(vehicle)の電気制御システムの部分の幾つかに影響を与える制御命令を出す局部PPE650によって、もしくは乗り物の作動に要求される特定のキー情報を複合化もしくは提供しない局部PPEいずれかによって、その後乗り物を作動することを阻まれる。

例--器具レンタル

本発明の使用を通じて、限定されない使用のために所定の器具を購入するより

は器具（VCR、テレビ、電子レンジ等）を手に入れて、１以上の使用の局面に従って料金を課されることを選ぶ顧客に、電子器具を「賃借」もしくは提供することができる。例えば、電子レンジは、品を用意するために使用される毎に、および／もしくは使用された時間に対して料金が課され得る。常にもしくは定期的にのいずれかで、テレホンジャックは、電子レンジ内に操作的に取り付けられた安いモデムに取り付けられ得る（あるいはモデムは、複数の品をサービスし、および／もしくは盗難警報機、照明および／もしくは温度制御などとして機能する位置に配置され得る）。あるいは、そのような器具は、シグナルを伝送および受け取るために、電力ケーブルによって形成されたネットワークを利用し得る。

定期的な間隔で、使用情報（概要の形式および／もしくは詳細な形式で）は、器具使用についての情報を集める遠隔情報ユーティリティに、自動的に送られ得る（ユーティリティは、特定のブランド、特定の器具のタイプ、および／もしくはブランドおよび／もしくはタイプの集まりをサービスし得る）。使用情報は、

VDE形式で送られ得る（例えば、VDEオブジェクト300）。情報ユーティリティそれ自体が課金機能を行わない場合、情報ユーティリティはその後、情報を金融手形交換所に配布し得る、もしくは各器具製造者および／もしくは貸し主（小売業者）に「属し」ている情報を、彼らもしくは彼らの代理人に送り得る。このようにして、新しい事業は器具をリースで使用することが可能となり得、器具のリースは車のリースと同様となり得る。

VDEをインストールすることにより、器具を安全識別によって管理することもでき得る（PIN、音声もしくは署名認識等）。これは、ユニットが使用される毎に、もしくは定期的基準に従って要求され得る。PPE650が、器具の機能の一部もしくは全ての使用を防ぐ１以上の命令を出した場合（もしくは複合化もしくは器具作動にとって重要な特定の情報を提供することに失敗した場合）、安全識別の使用の失敗もしくは適時基準に従った使用の失敗は、器具を不能にでき得る。この特徴は、電子器具の盗難のしやすさを大いに減少させ得る。さらに、VDEを提携した使用とは、家もしくはビジネスの場の制御位置にある、VDE安全サブシステムを備えた所定の器具におけるVDE安全サブシステムの「登録」である。この

制御位置はまた、VDE遠隔通信および／もしくは中央化された管理（例えば、所定の映画、歌、チャンネル、ゲーム等がＲ指定であることを示すデータの認識を通じて、子どもがＲ指定の映画をテレビもしくはビデオカセットいずれかで観ることを制限すること、および親が子供に観ることもしくは聴くことを制限することが可能にすることを含む）に責任がある。そのような制御位置は、例えば、水、ガス、電気の消費量、電話使用量等（そのような消費を測定および／もしくは制御するための制御手段内に一体化されたPPE650の使用を通じて、もしくは非VDEシステムによって生成され、例えば処理、使用制御（例えば、使用制限）、および／もしくは課金のためのVDE安全サブシステムに配送される、１以上のシグナルを通じてのいずれか）の情報を集め、そのような情報を１以上のユーティリティに伝送し、VDE安全化電子通貨および／もしくはクレジット等を用いて、そのような消費に対して支払い得る。

加えて、使用のための１以上の予算をVDEによって管理することができ、VDEは特定の賃借された器具の、例えばデューティサイクルによって指定されたよりも多いコピーを写真式複写機を用いて作ってしまうなどの、器具の機能不全につながる不適切で過剰な使用を防止し得る。そのような不適切な使用は、ユーザがよりしっかりしたモデルへとアップグレードするべきことを知らせる、例えばディスプレイパネル上もしくはテレビ画面上のメッセージとなって、もしくは中央手形交換所からの通信という形式のメッセージとなって現れる。

本発明は、最も実際的で好適な実施態様と現在考えられているものと関連させて説明されてきたが、本発明は、開示された実施態様に制限されるものではなく、それどころか、添付された請求項の意図および範囲に含まれる、多様な改変および同等のアレンジメントを含むことを意図する。

【図１】

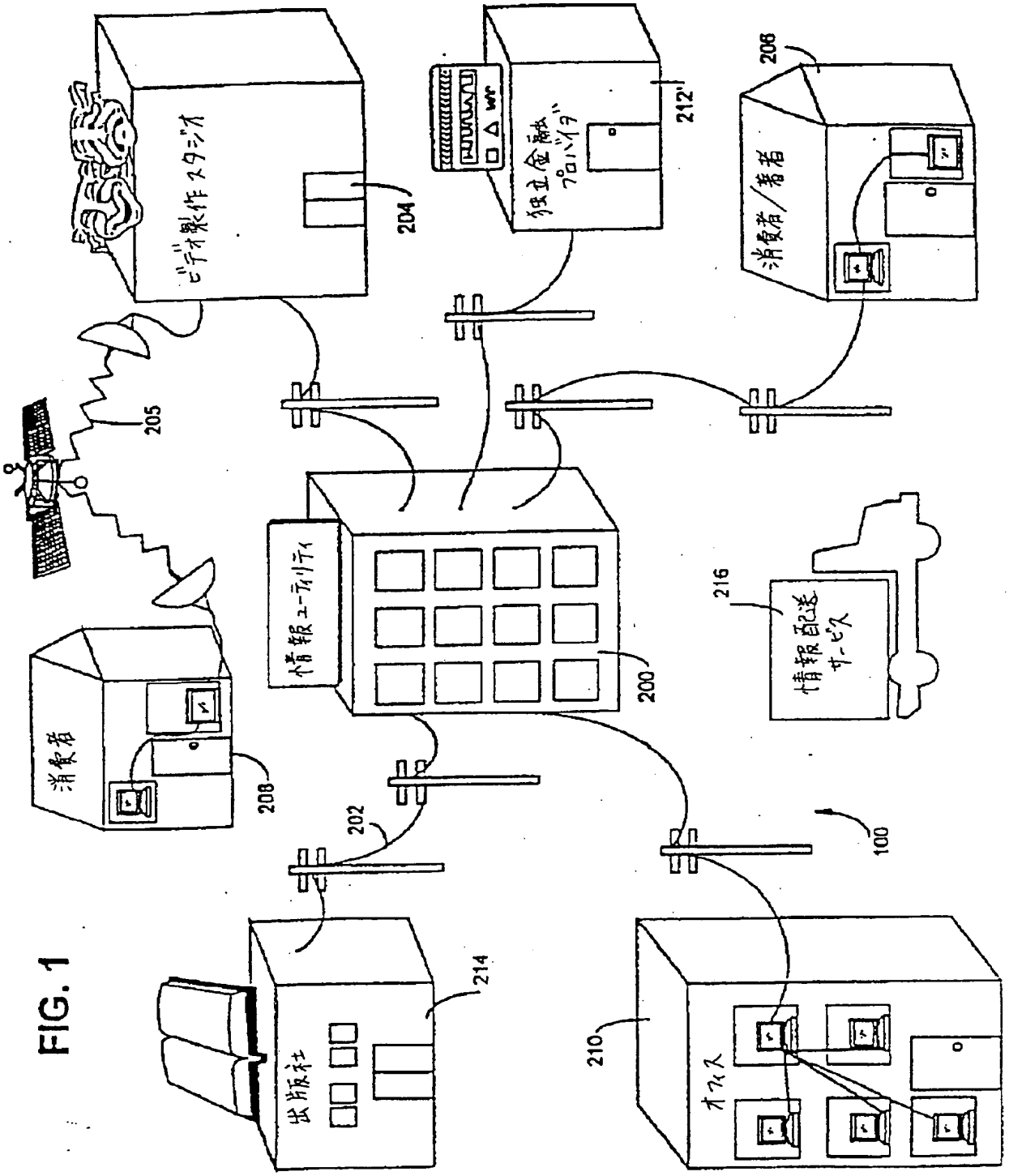

ビデオ製作スタジオ
204
独立金融プロバイダ
212'
206
消費者／著者
205
情報ユーティリティ
200
216
情報配送サービス
消費者
208
202
100
出版社
214
210
オフィス

FIG. 1

【図１】

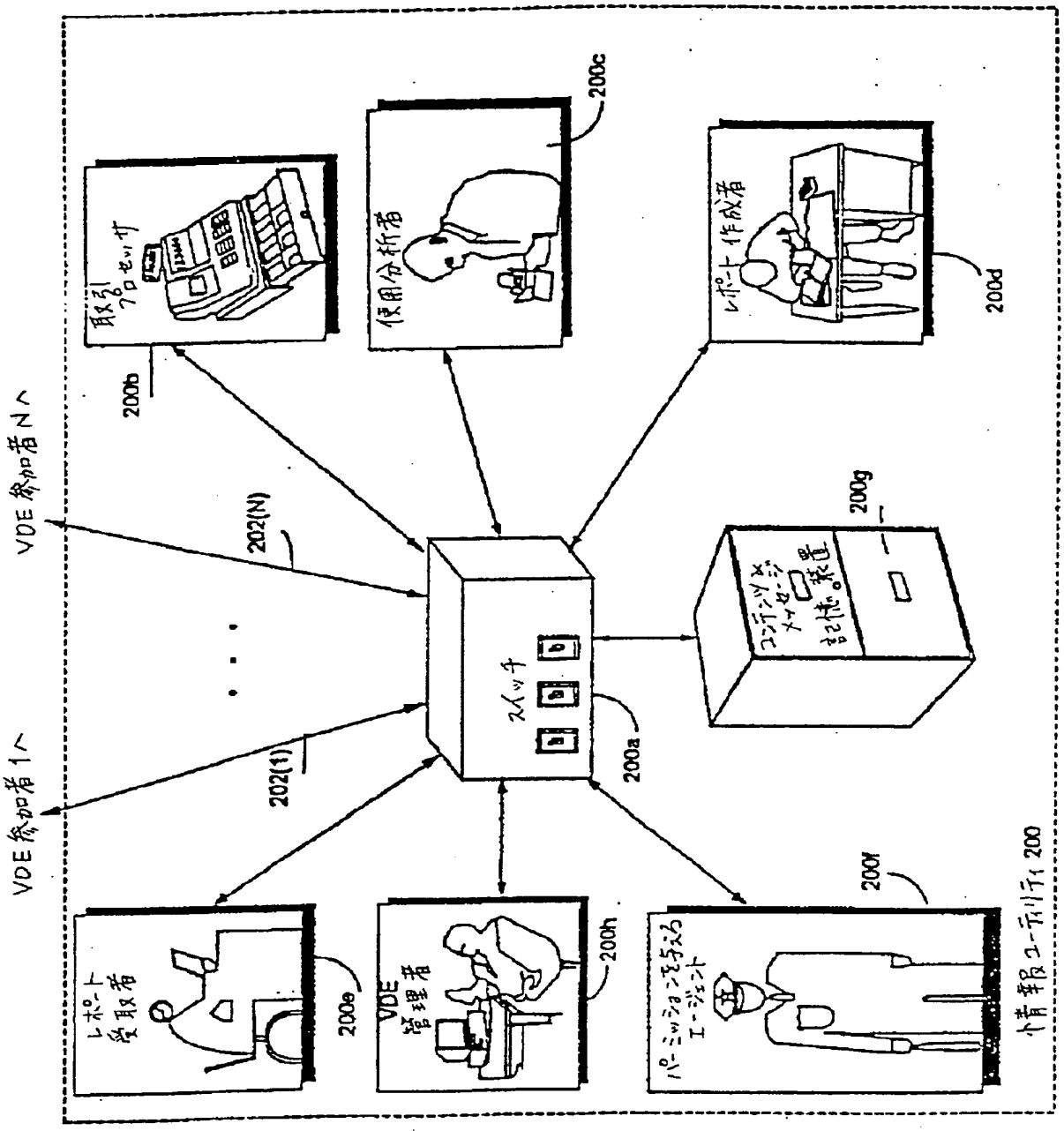
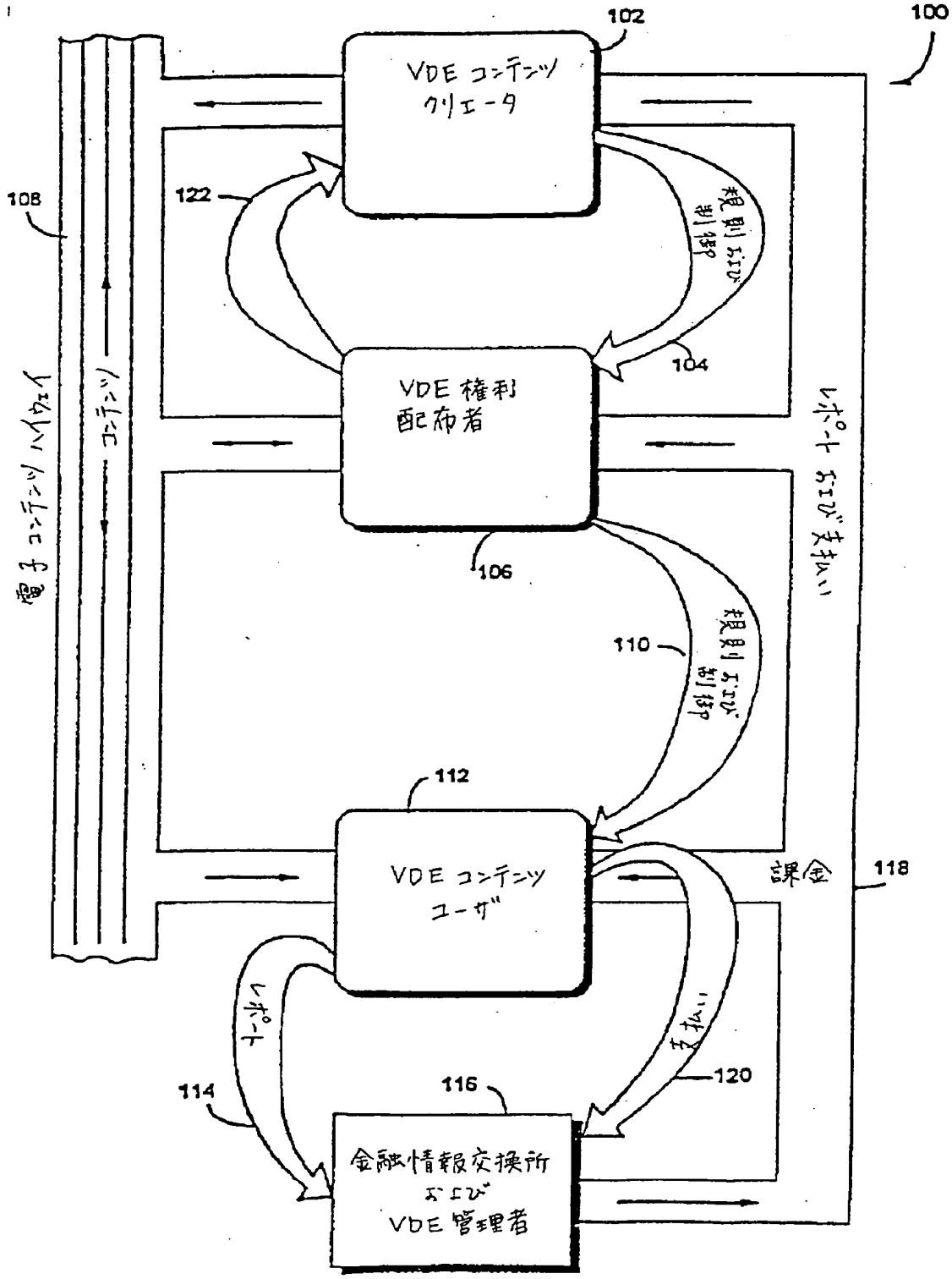

VDE参加者１
VDE参加者Ｎ
202(1)
202(N)
スイッチ
200a
200b
200c
200d
200e
200f
200g
200h
情報ユーティリティ 200
レポート受取者
VDE管理者
レポート作成者
使用分析者
取引プロセッサ
コンテンツ・メッセージまたは秘密裏

FIG. 1A

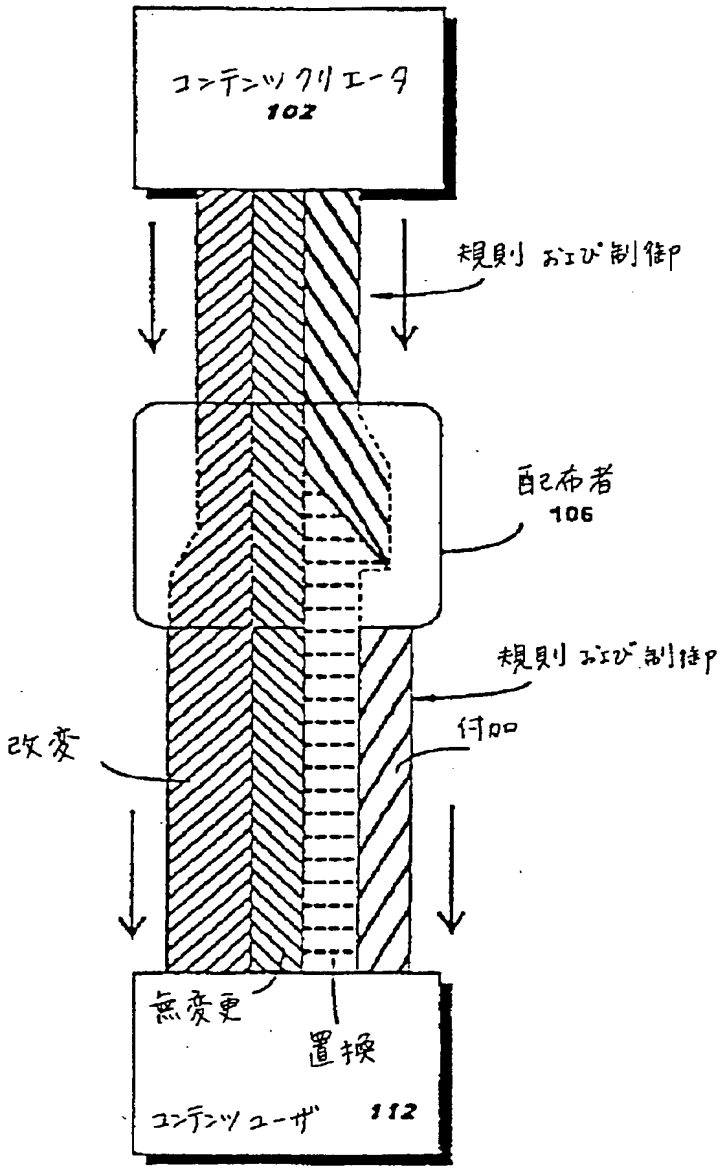
【図２】

FIG. 2


100
102
VDE コンテンツ クリエータ
122
権利ラベル
104
VDE 権利配布者
106
108
電子コンテンツハイウェイ
コンテンツ
ネットワーク
110
権利ラベル
112
VDE コンテンツユーザ
課金
118
ネットワーク
支払い
120
114
116
金融情報交換所および VDE 管理者

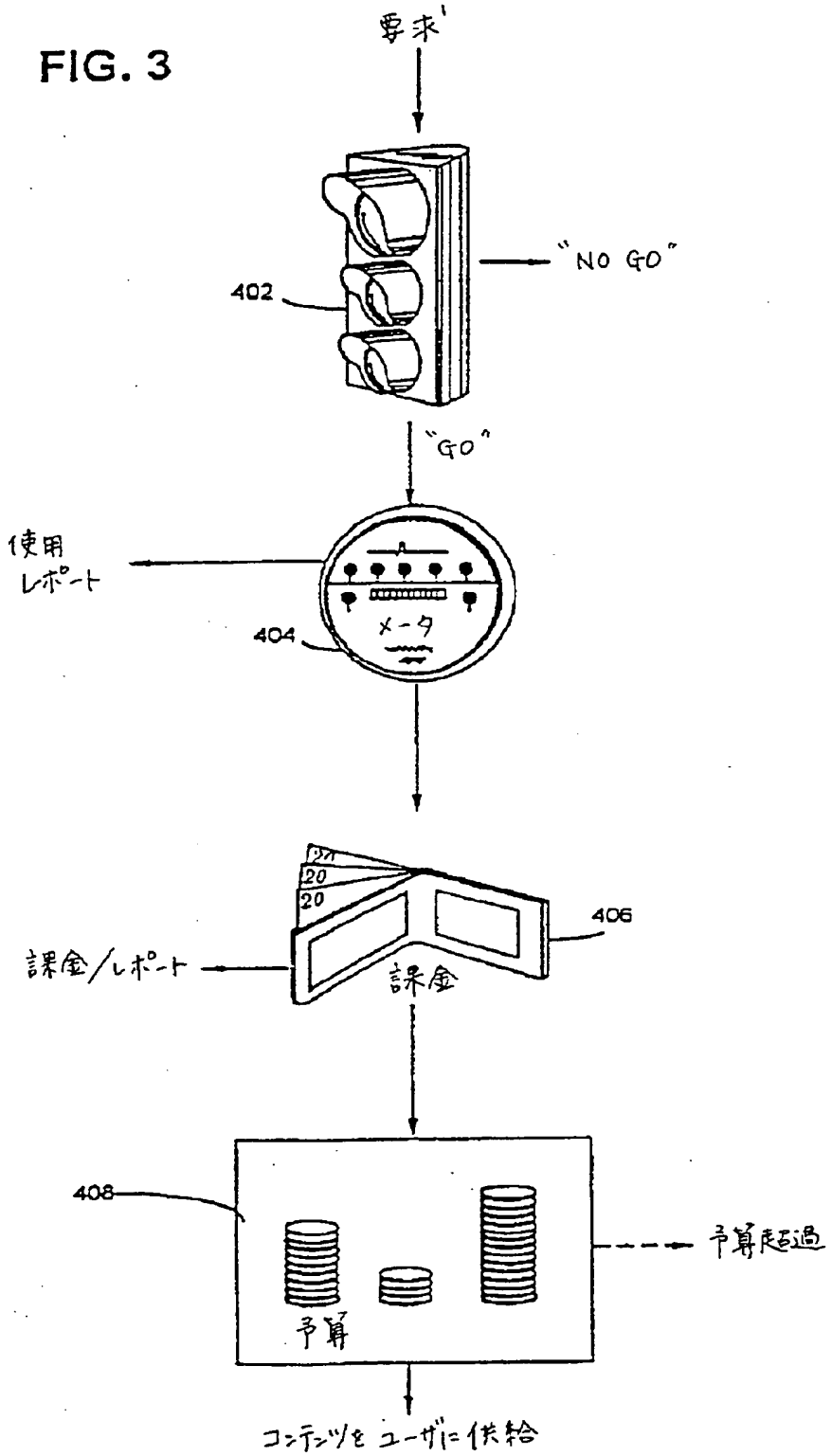
【図２】

FIG. 2A


コンテンツクリエータ
102
規則および制御
配布者
106
規則および制御
付加
改変
無変更
置換
コンテンツユーザ
112

【図３】

FIG. 3


要求
"NO GO"
402
"GO"
使用
レポート
メータ
404
20
20
20
406
課金/レポート
課金
408
予算超過
予算
コンテンツをユーザに供給

【図４】

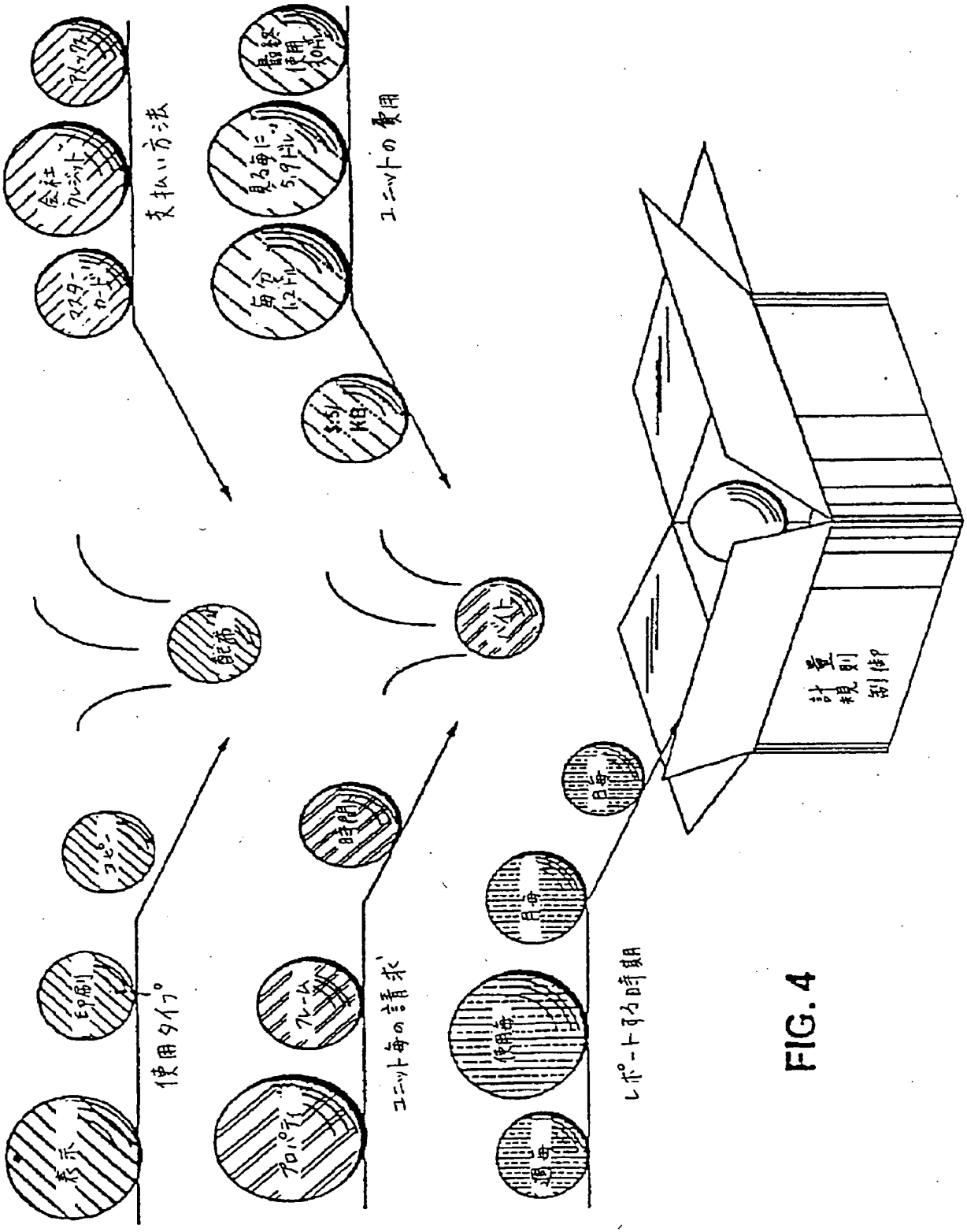
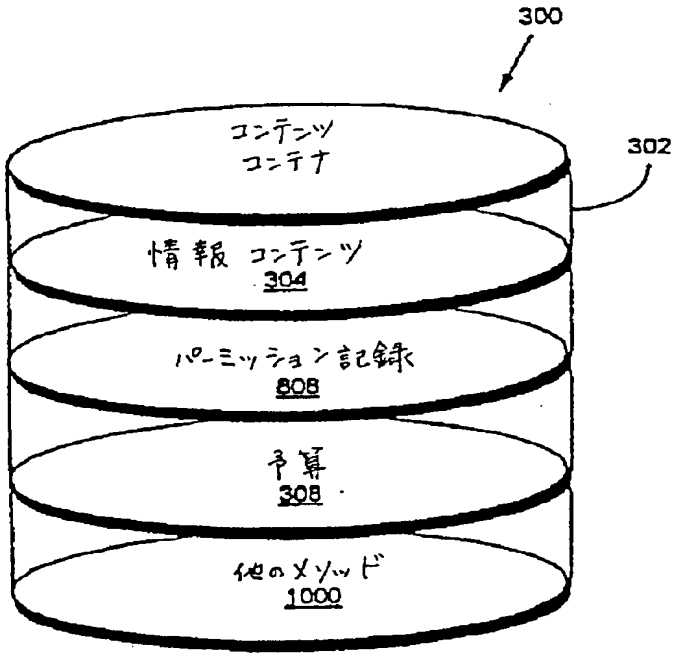


FIG. 4

【図５】

FIG. 5A


300
302
コンテンツ
コンテナ
情報 コンテンツ
304
パーミッション記録
606
予算
308
他のメソッド
1000

【図５】

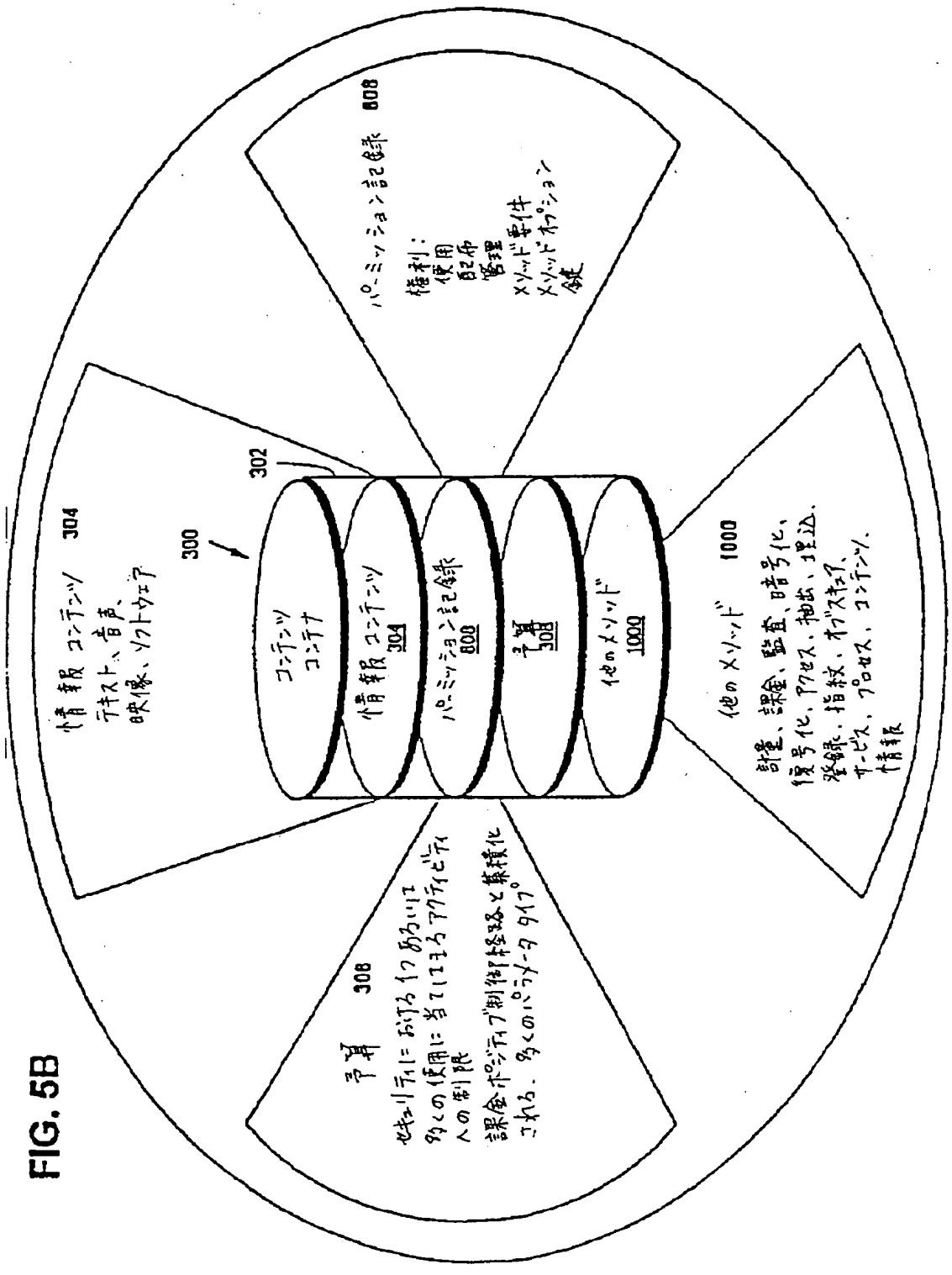
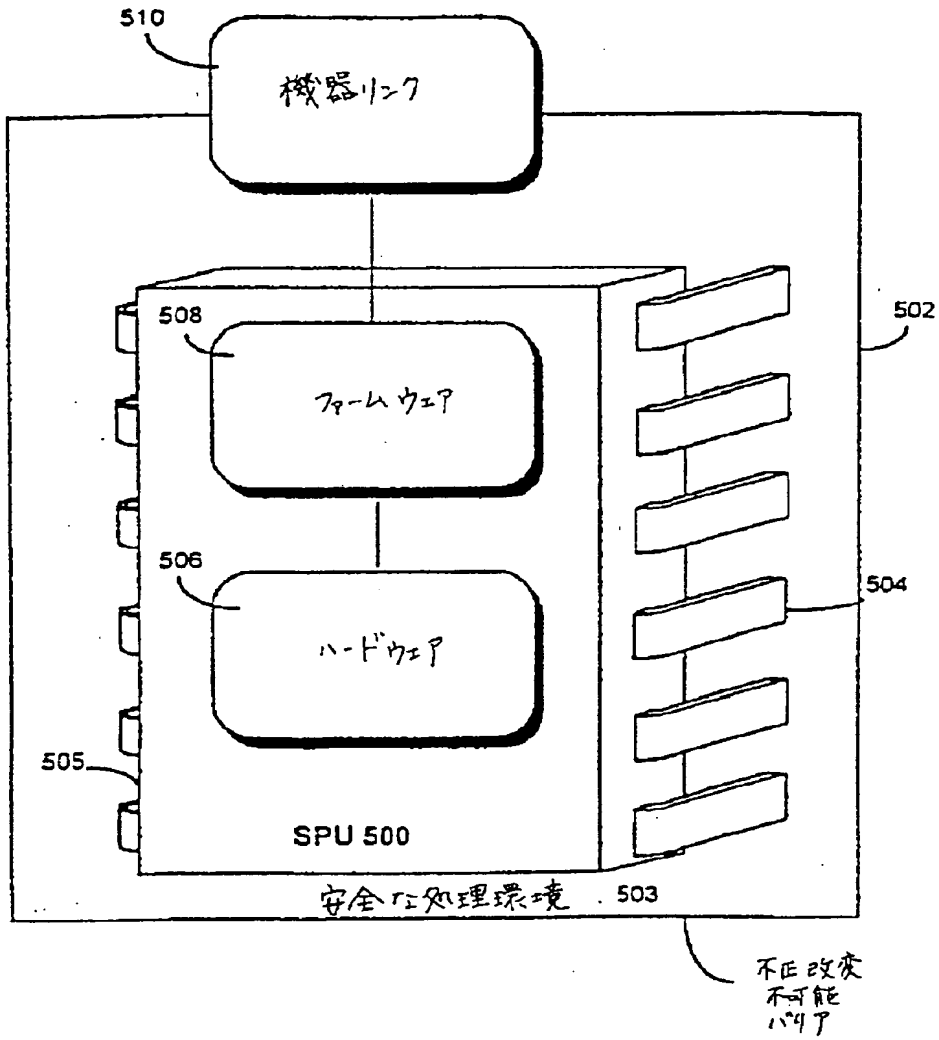

300
302
コンテンツ
コンテナ
情報コンテンツ
304
パーミッション記録
800
予算
308
他のメソッド
1000
情報コンテンツ 304
テキスト、音声、
映像、ソフトウェア
パーミッション記録 808
権利：
使用
配布
管理
メソッド毎1件
メソッドオプション
他のメソッド 1000
部屋、課金、監査、暗号化、
復号化、アクセス、抽出、埋込、
登録、指紋、オブスキュア、
サービス、プロセス、コンテンツ、
情報
予算 308
セッション おける 1つ あるいは
多くの使用に当てはまる アクティビティ
への制限
課金ポリシーおよび制御経路と集積化
これら、多くのパラメータ タイプ

FIG. 5B

【図６】

FIG. 6


510
機器リンク
508
ファームウェア
506
ハードウェア
505
SPU 500
502
504
安全な処理環境 503
不正改変
不可能
バリア

【図７】

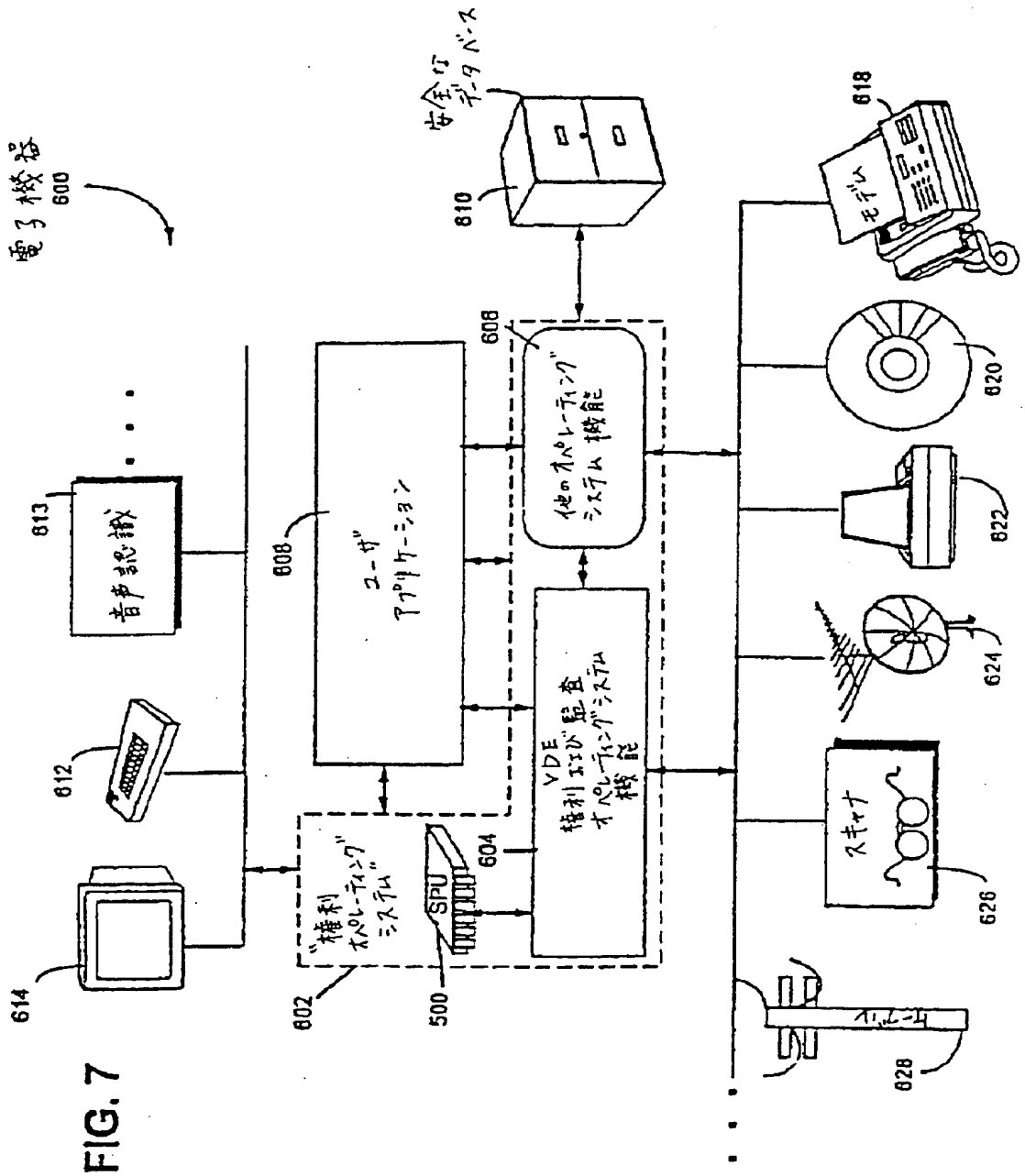
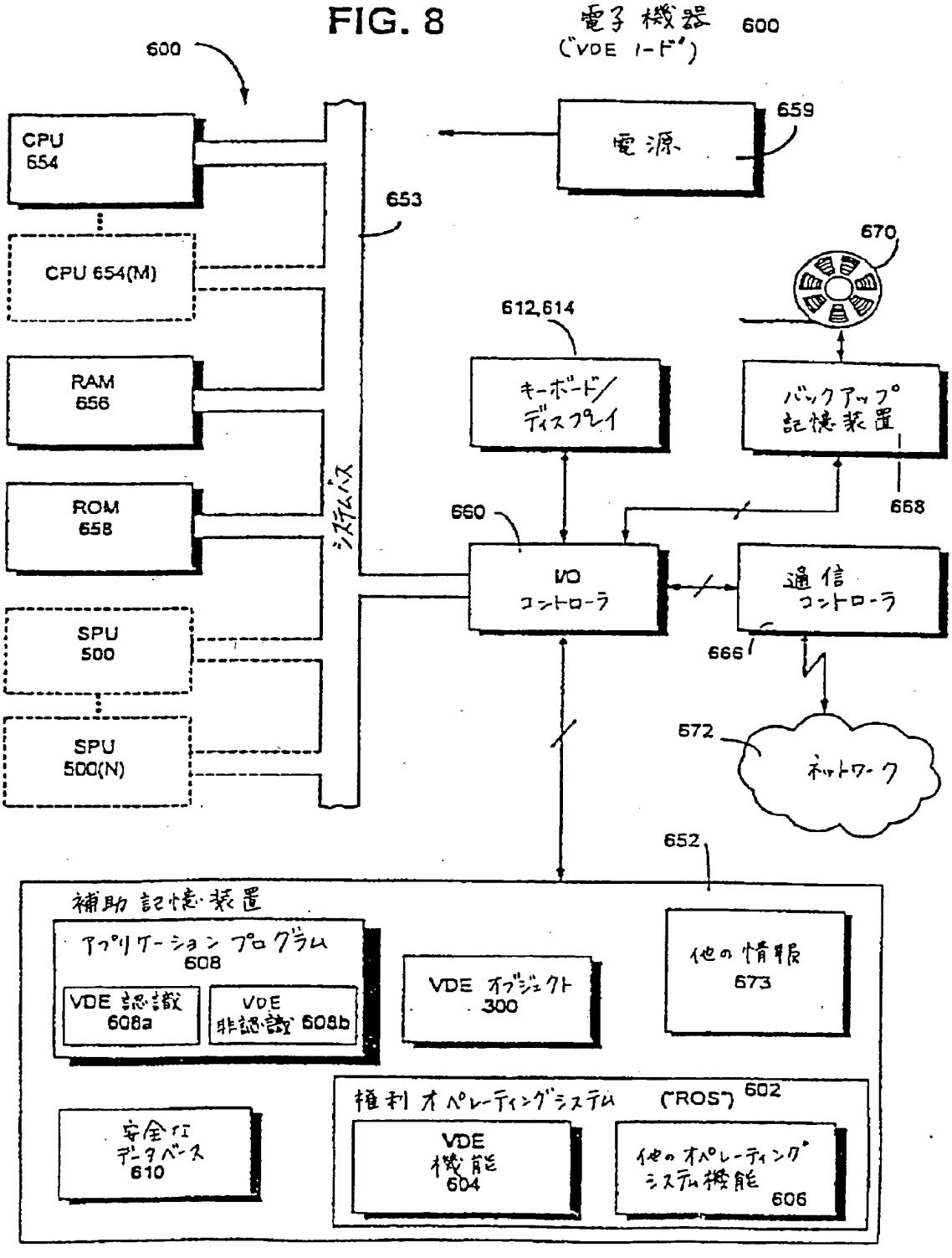

電子機器
600
安全DTD データベース
810
618
モデム
608
ユーザ アプリケーション
他のオペレーティング システム 機能
620
622
624
626
628
613
音声認識
612
614
602
"権利オペレーティング システム"
SPU
500
604
VDE 権利エリア監査 オペレーティング システム 機能
スキャナ

FIG. 7

［図８］

FIG. 8


電子機器 600
(VDE ノード)
600
CPU 654
CPU 654(M)
RAM 656
ROM 658
SPU 500
SPU 500(N)
システムバス
653
電源
659
670
612,614
キーボード/ディスプレイ
バックアップ記憶装置
668
660
I/O コントローラ
通信コントローラ
666
672
ネットワーク
652
補助記憶装置
アプリケーションプログラム 608
VDE 認識 608a
VDE 非認識 608b
VDE オブジェクト 300
他の情報 673
安全なデータベース 610
権利オペレーティングシステム (ROS) 602
VDE 機能 604
他のオペレーティングシステム機能 606

【図９】

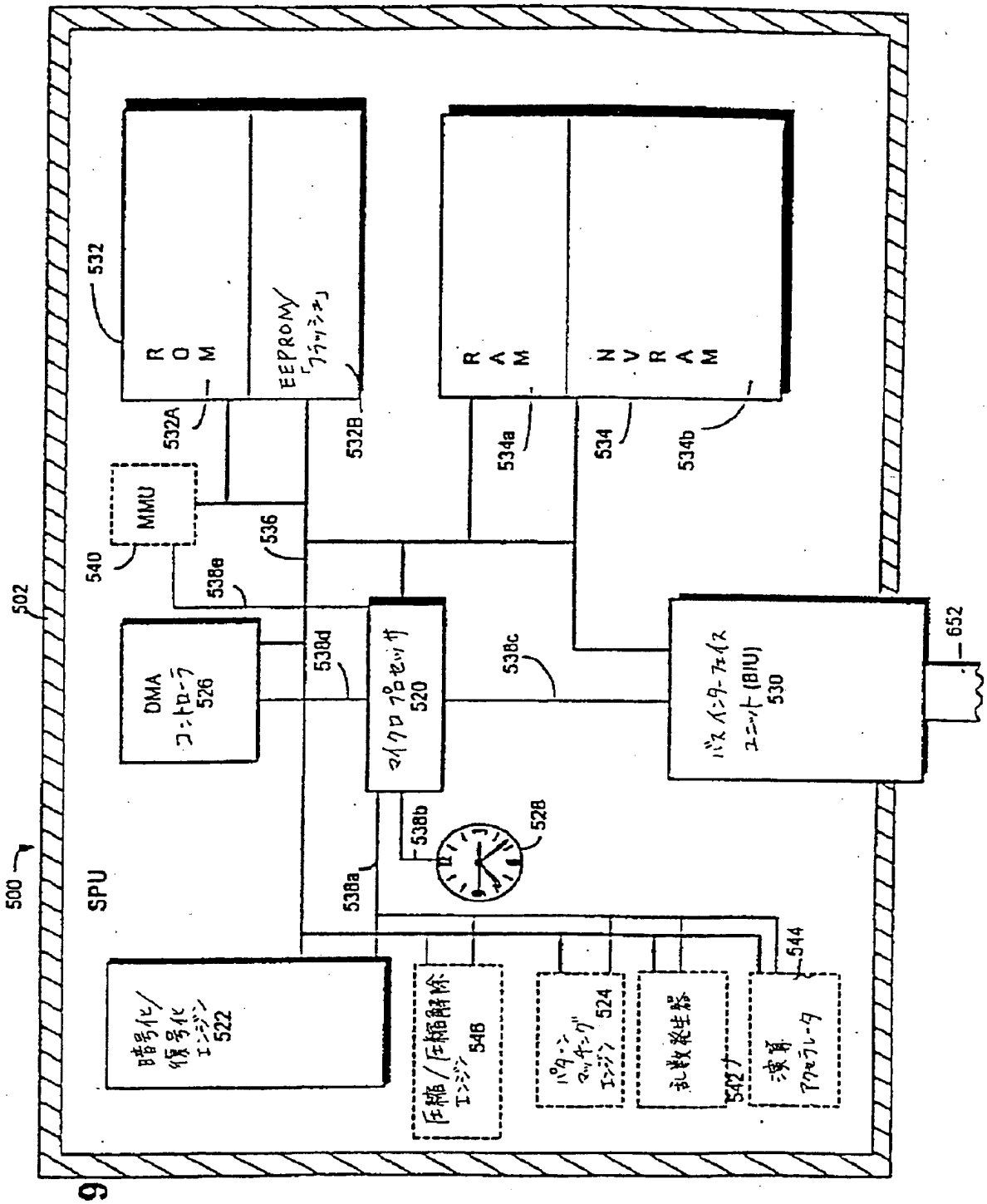

500
SPU
502
532
R O M
EEPROM/フラッシュ
532A
532B
R A M
N V R A M
534a
534
534b
MMU
540
536
538a
DMA コントローラ 526
538d
マイクロプロセッサ 520
538c
バスインターフェイス ユニット (BIU) 530
652
538b
528
538a
暗号化/復号化 エンジン 522
圧縮/圧縮解除 エンジン 546
ハフマン コーディング エンジン 524
乱数発生器 542
544
演算アクセラレータ

FIG. 9

【図１０】

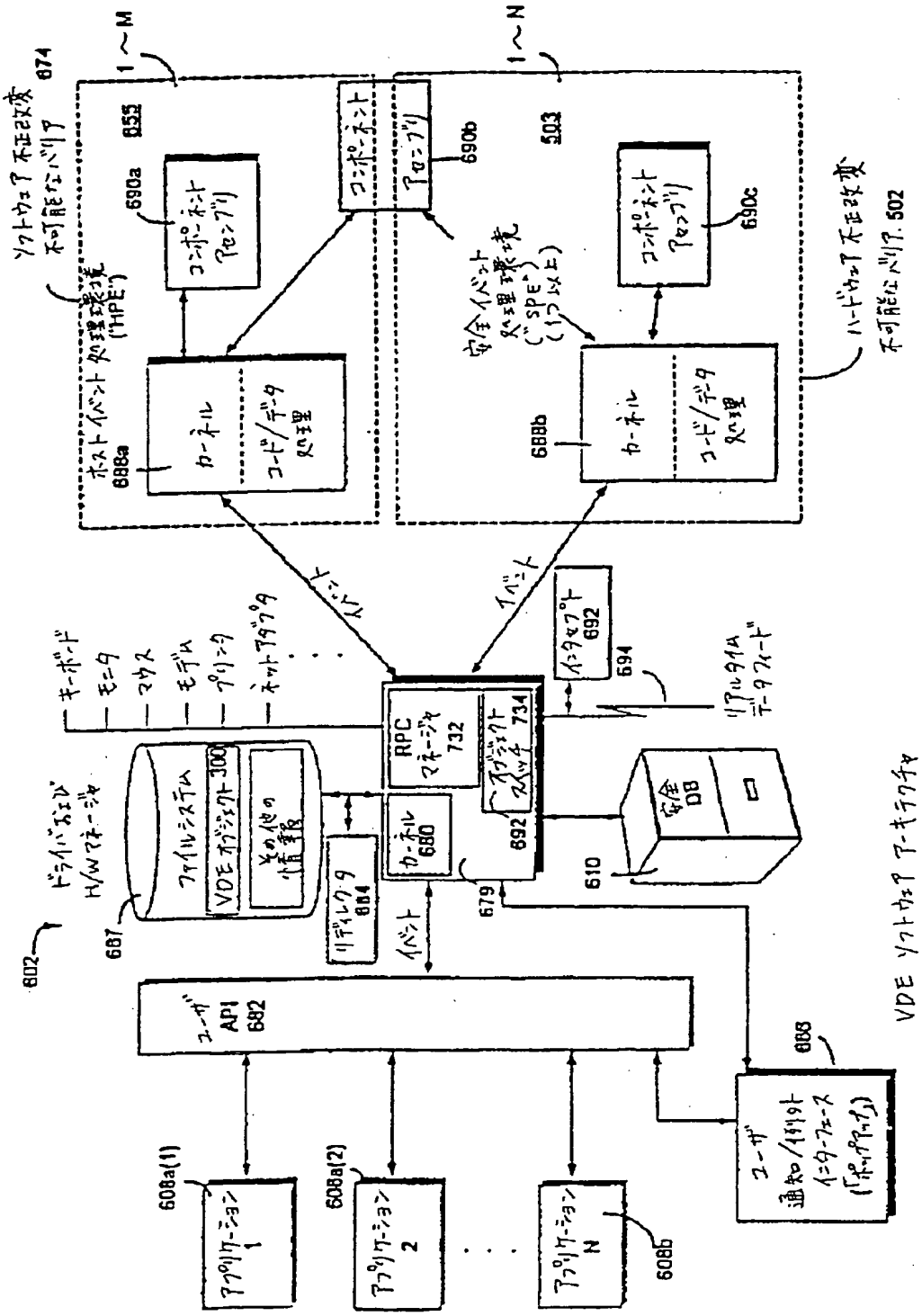

ソフトウェア不正改変
不可能なパリア
674
1～M
1～N
ホストイベント処理環境
("HPE")
655
690a
コンポーネント
アセンブリ
690b
503
コンポーネント
アセンブリ
690c
安全イベント
処理環境
("SPE")
(1つ以上)
ハードウェア不正改変
不可能なパリア. 502
688a
カーネル
コード/データ
処理
688b
カーネル
コード/データ
処理
イベント
イベント
キーボード
モニタ
マウス
モデム
プリンタ
ネットワーク
インタフェース
692
694
リアルタイム
データフィード"
RPC
マネージャ
732
オブジェクト
スペース
734
ドライバおよび
H/Wマネージャ
602
ファイルシステム
VDEオブジェクト
300
その他の
情報
687
カーネル
680
692
リダイレクタ
684
イベント
679
安全
DB
610
ユーザ
API
682
608a(1)
608a(2)
608b
アプリケーション
1
アプリケーション
2
アプリケーション
N
ユーザ
通知/制御
インターフェース
(「ポップアップ」)
688
VDE ソフトウェア アーキテクチャ

FIG. 10

【図１１】

FIG. 11C

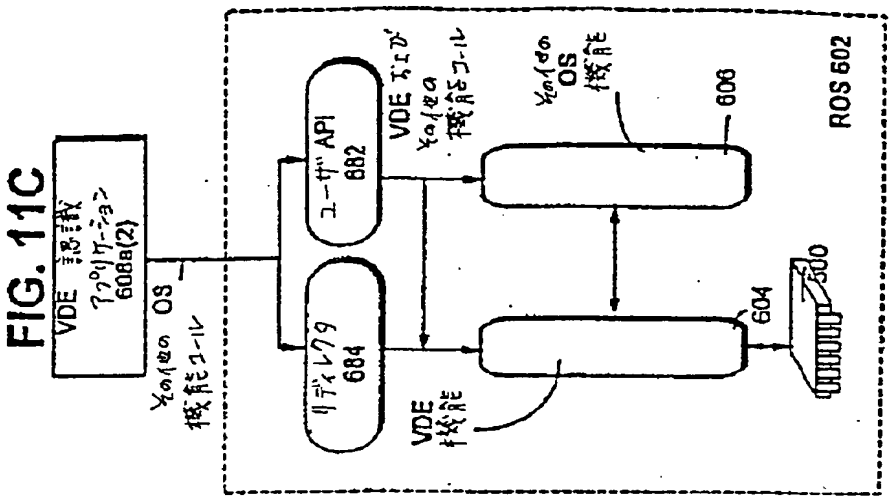


FIG. 11B

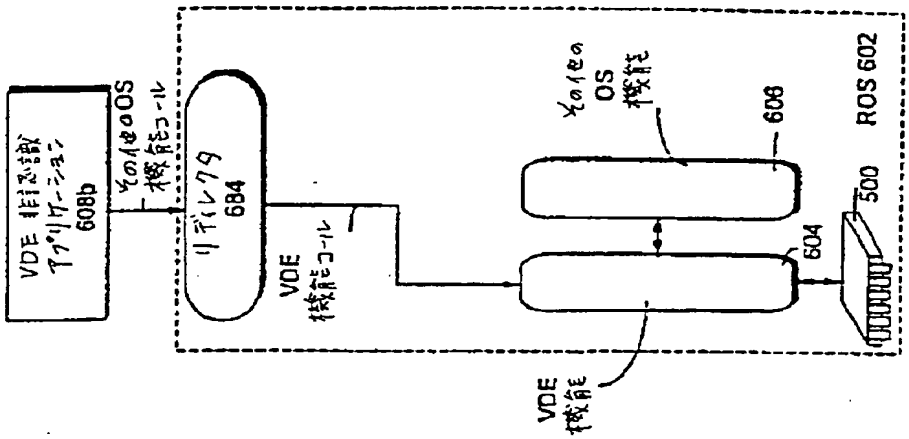
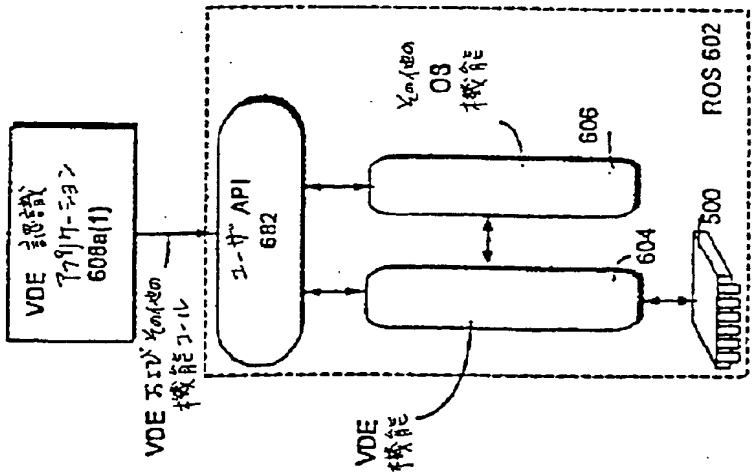


FIG. 11A



【図１１】

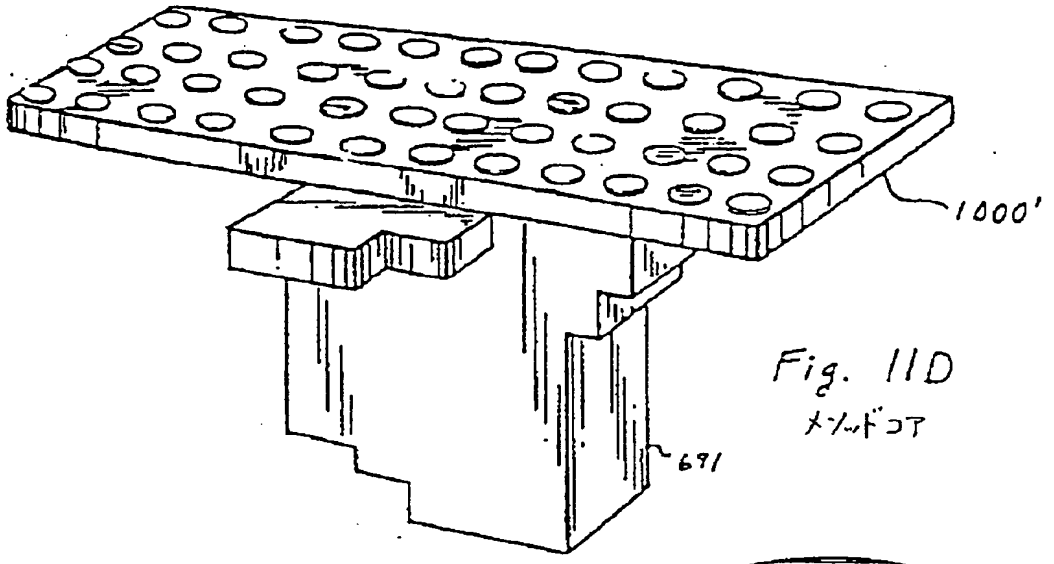


Fig. 11D
メソッドコア

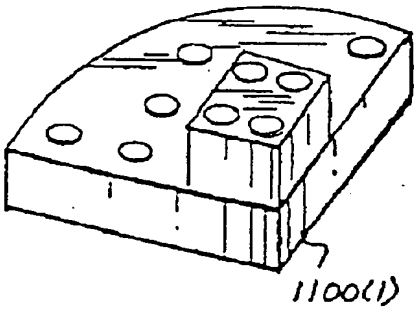


Fig. 11E
DTDを有するロードモジュール

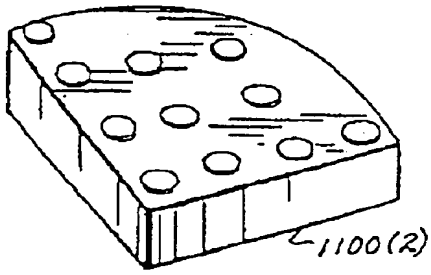


Fig. 11F
ロードモジュール

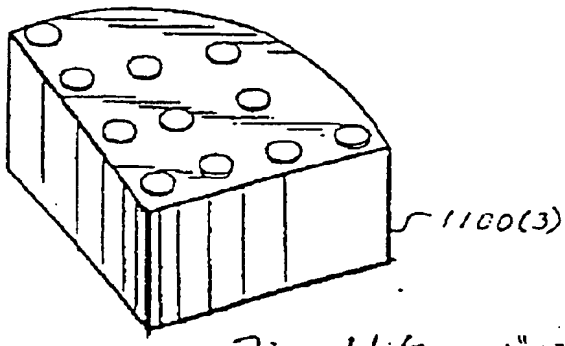


Fig 11G ロードモジュール

【図１１】

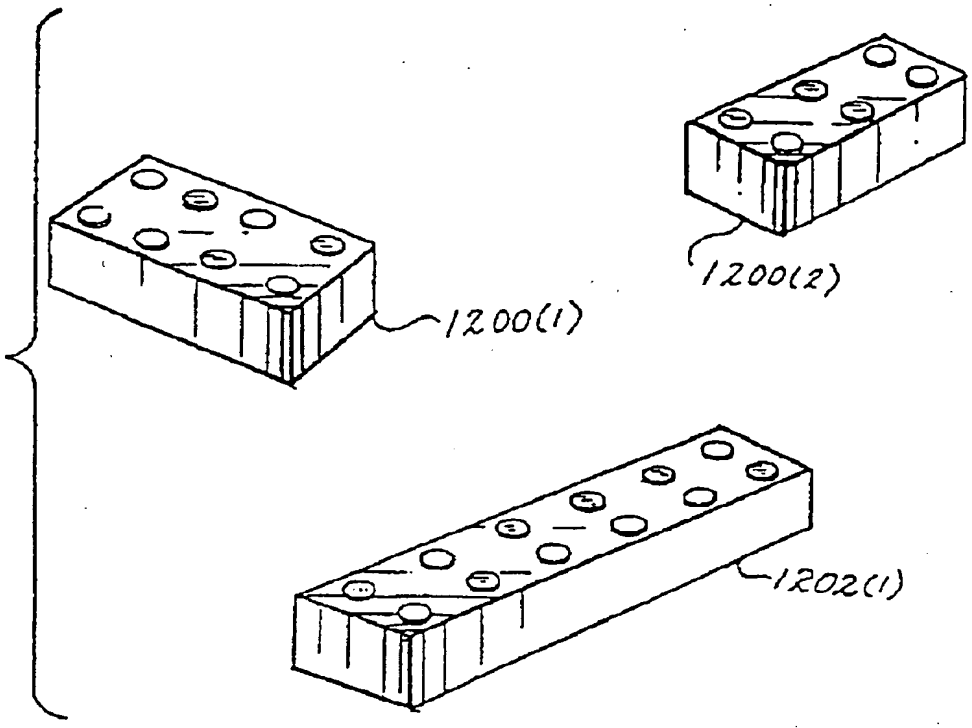
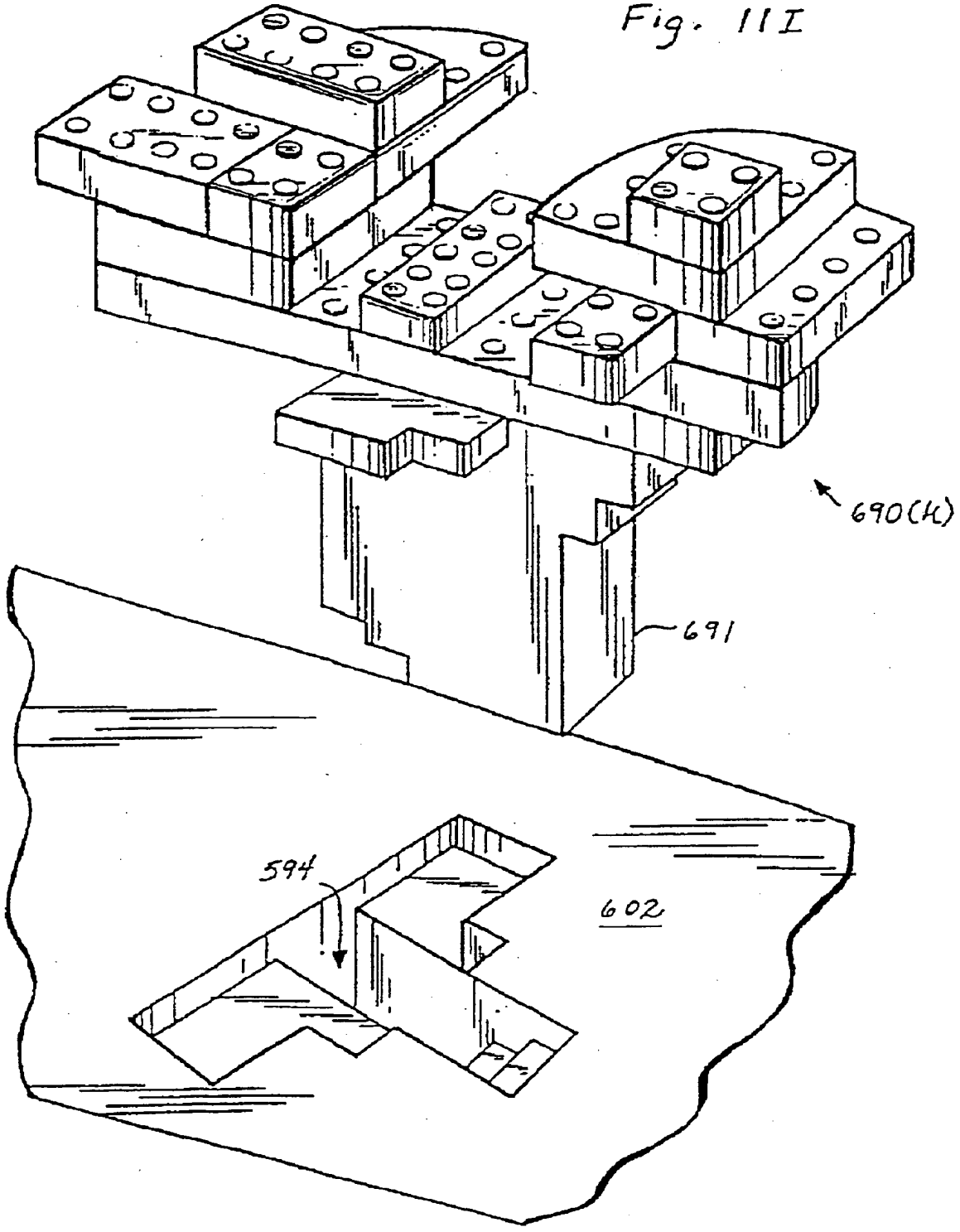


Fig. 11H
データストラクチャ

【図１１】

Fig. 11I



【図１１】

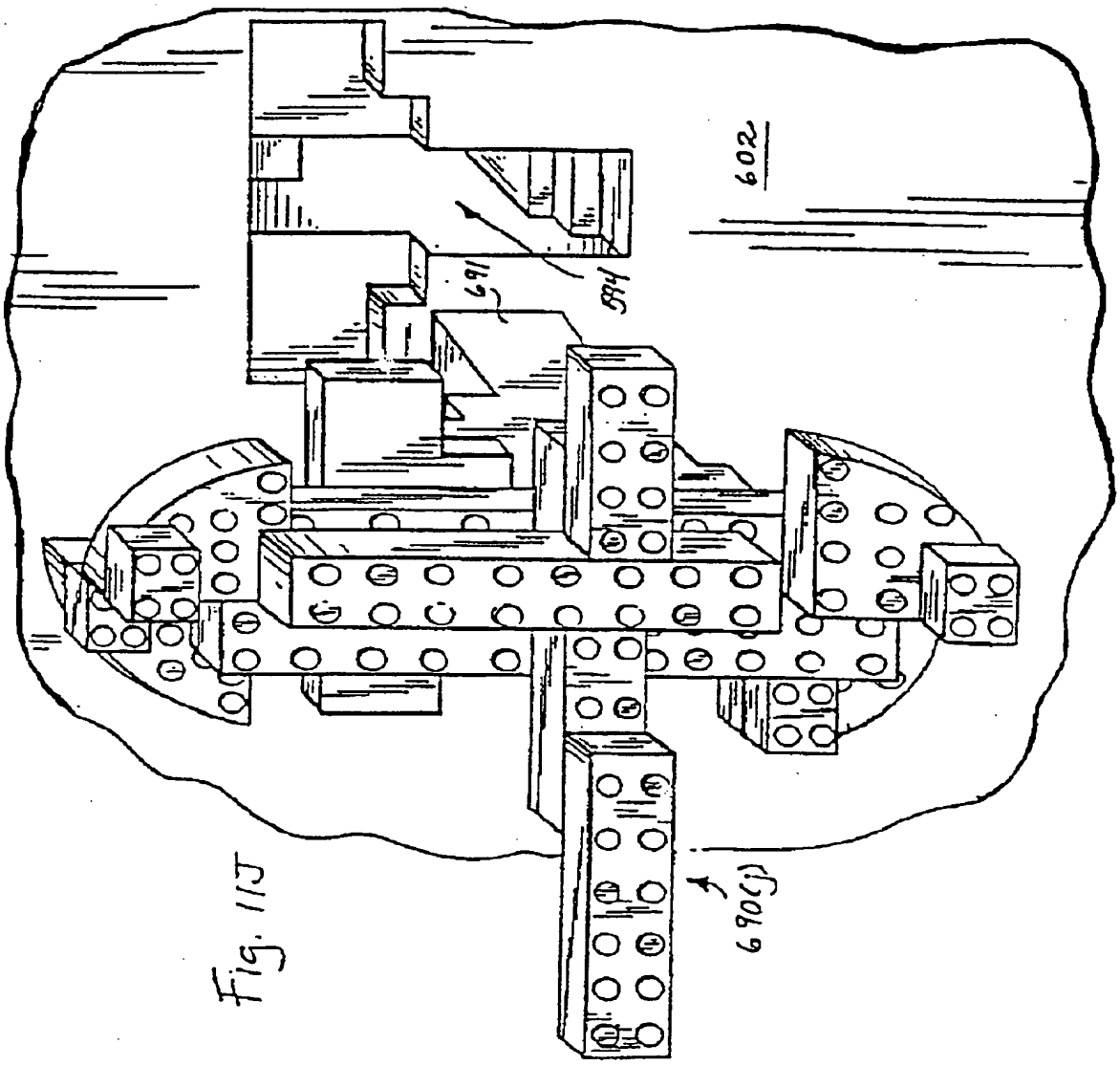
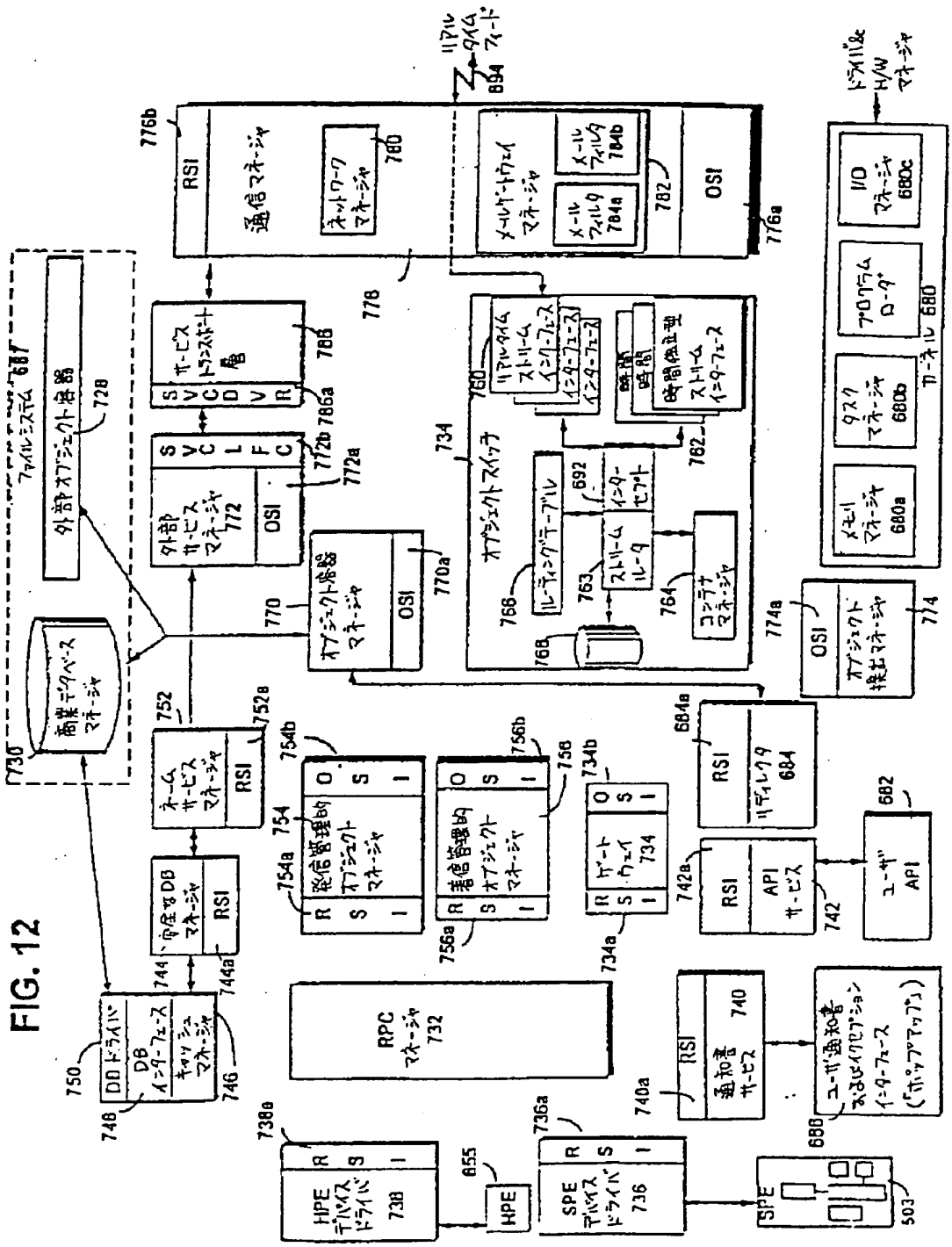


Fig. 11J

【図１２】

FIG. 12


RSI
通信マネージャ
776b
776a
OSI
ネットワーク マネージャ
780
メールゲートウェイ マネージャ
メール フィルタ 784a
メール フィルタ 784b
782
ドライバ& H/W マネージャ
I/O マネージャ 680c
プロトコル ローダ
タスク マネージャ 680b
メモリ マネージャ 680a
カーネル 680
778
外部サービス マネージャ 772
外部サービス トランスポート層
772a
772b
785a
785b
外部オブジェクト参照
728
ファイルシステム 687
商業データベース マネージャ
730
オブジェクト マネージャ
770
770a
オブジェクト スイッチ
734
リアルタイム ストリーム インターフェース
760
時間依存型 ストリーム インターフェース
782
ルーティング テーブル
766
692
インターセプト
763
ストリーム ルータ
764
コンテナ マネージャ
768
774a
OSI
オブジェクト検証マネージャ
714
684a
RSI
リダイレクタ 684
682
ユーザ API
742
RSI
API サービス
742a
ゲート カウンタ 734
734a
734b
送信管理補助 オブジェクト マネージャ
754
754a
754b
受信管理補助 オブジェクト マネージャ
756a
756b
ネーム サービス マネージャ
752
752a
DB マネージャ
744
744a
DB ドライバ
DB インターフェース
748
750
RPC マネージャ 732
RSI
通知書 サービス 740
740a
ユーザ通知書およびインターフェース（ポップアップ）
688
HPE ドライバ 738
738a
HPE
655
SPE ドライバ 736
736a
SPE
503

【図１２】

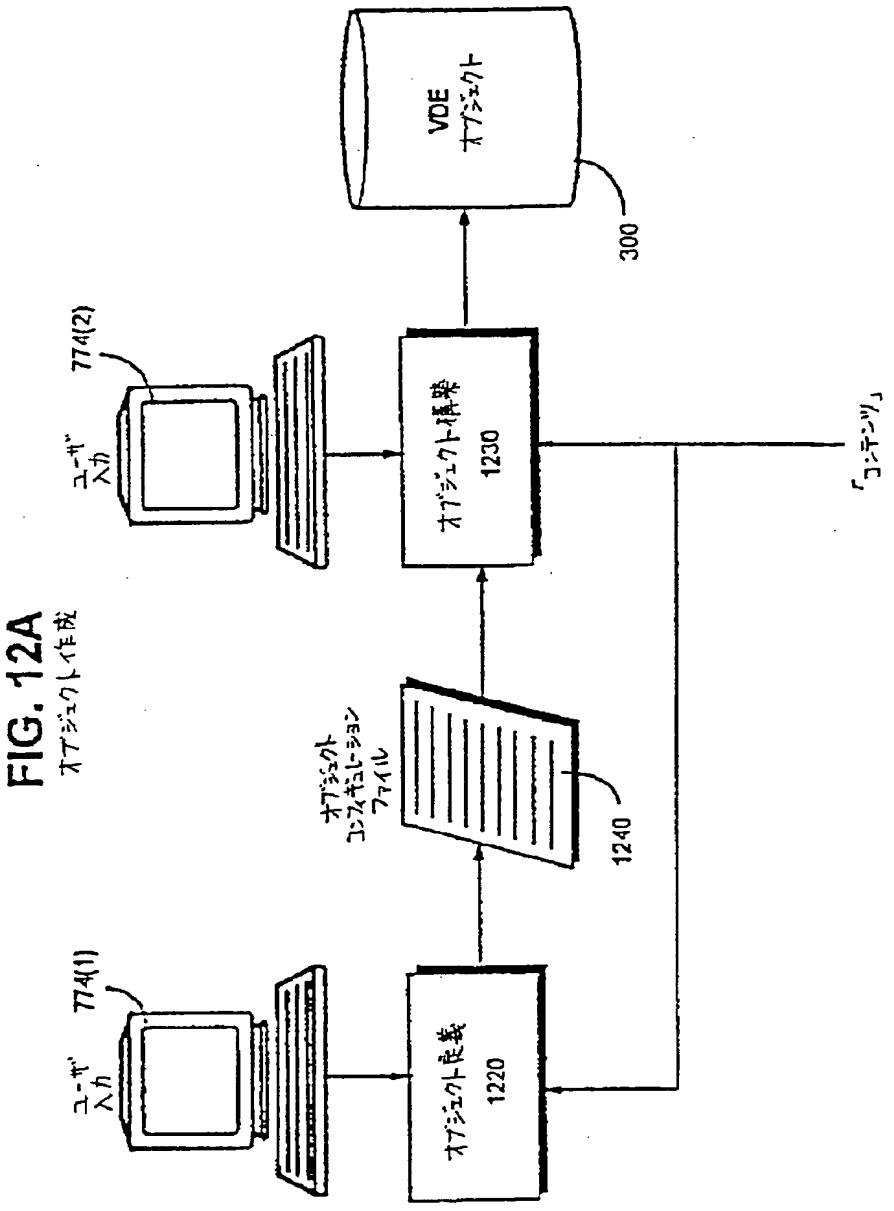
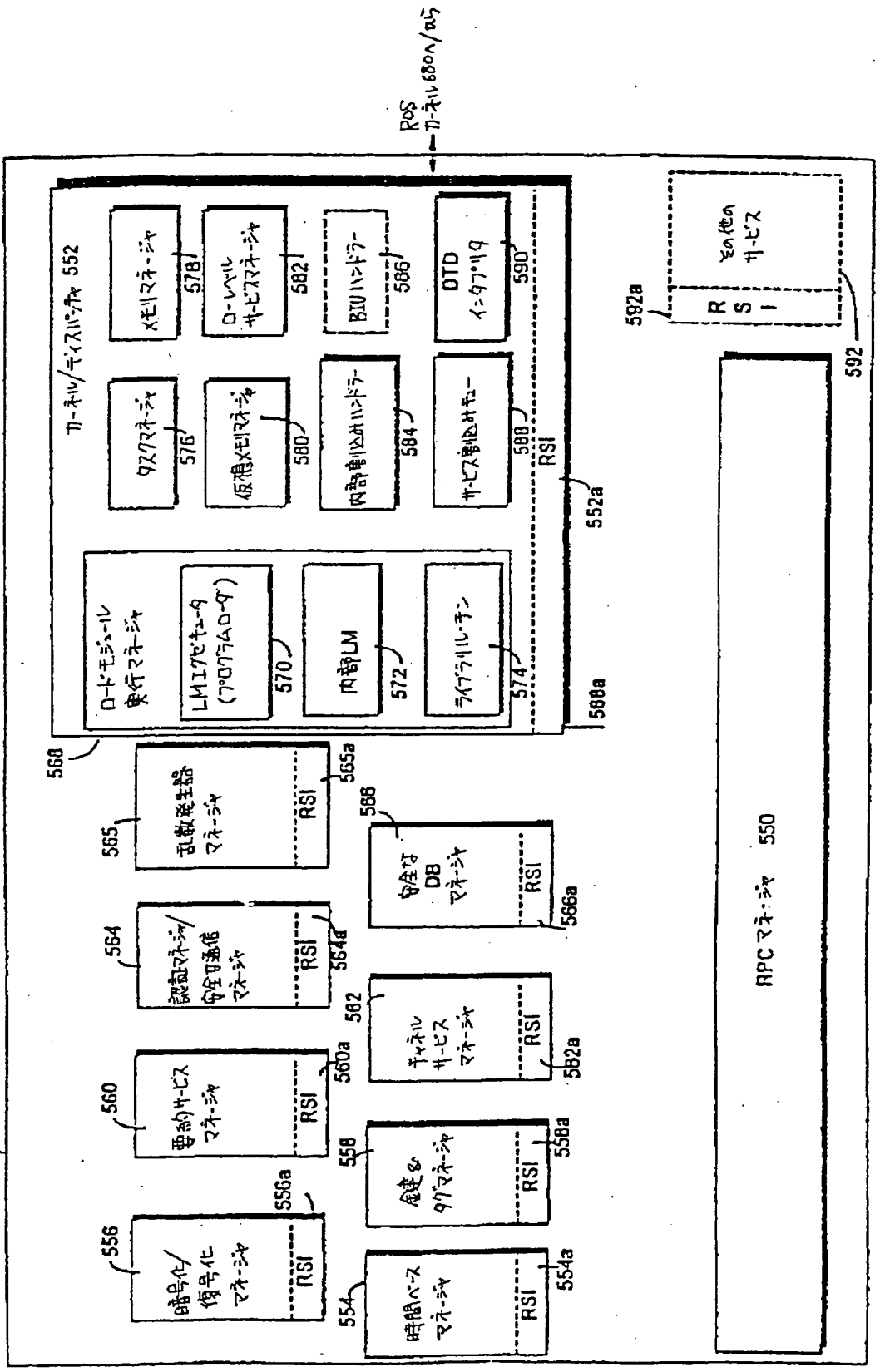


FIG. 12A
オブジェクト作成

【図13】

FIG. 13

プロテクト下の処理環境 650



【図１４】

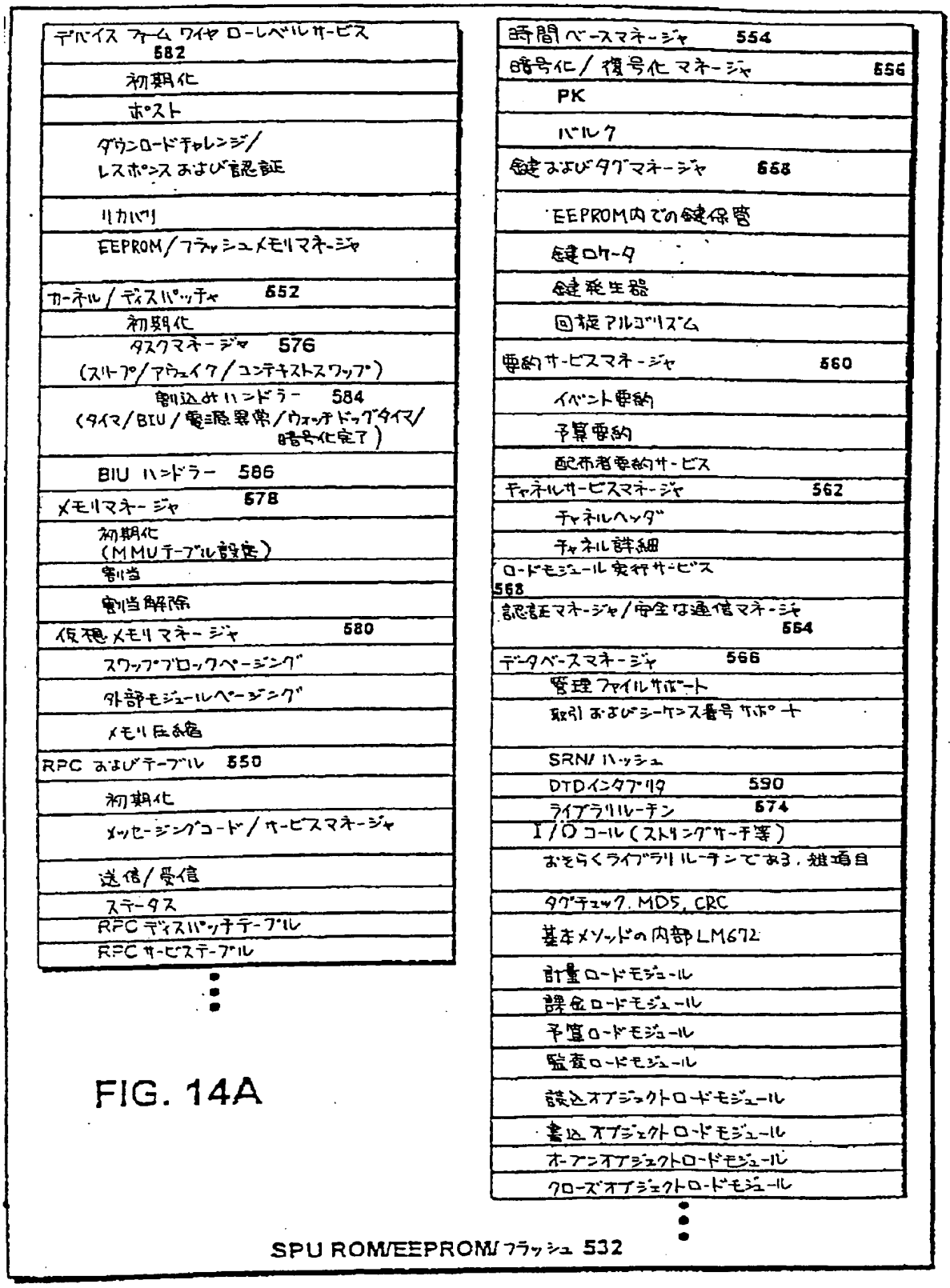
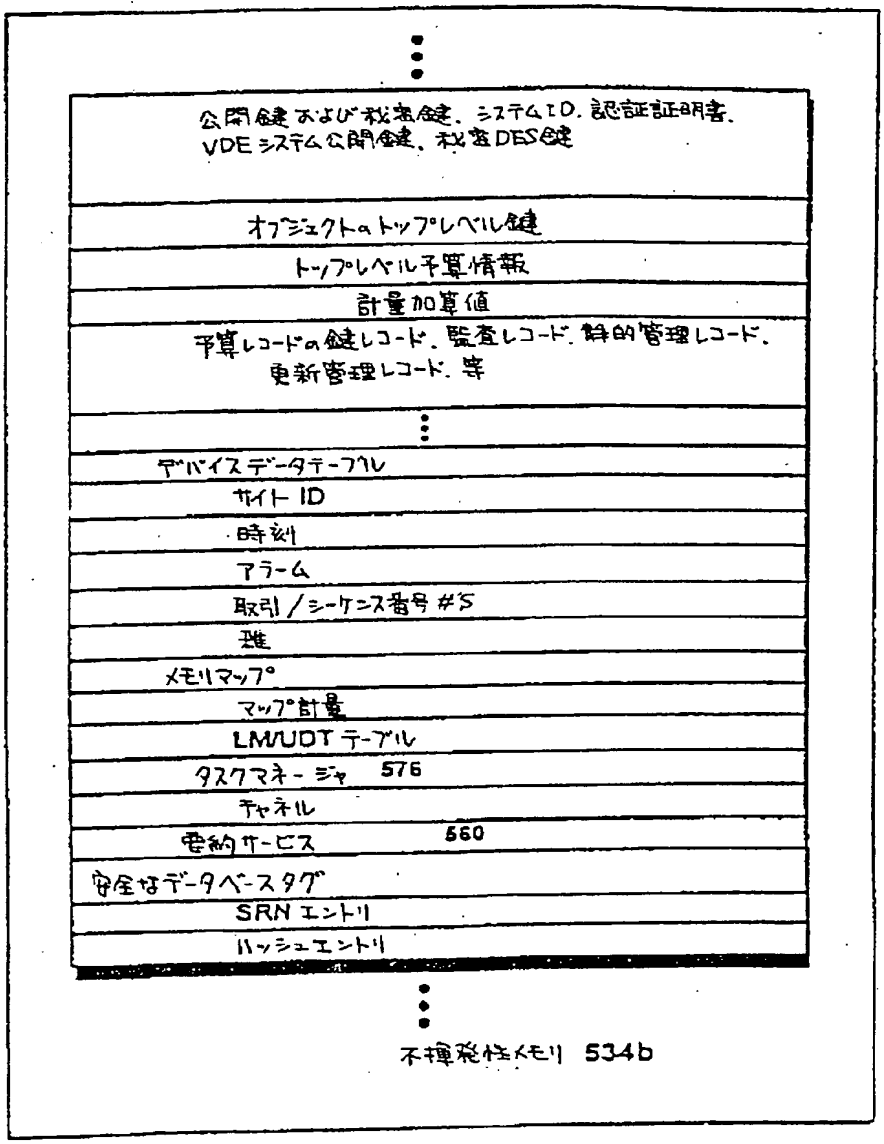

デバイス フォーム ワイヤ ローレベルサービス 582
初期化
ポスト
ダウンロードチャレンジ/レスポンスおよび認証
リカバリ
EEPROM/フラッシュメモリマネージャ
カーネル/ディスパッチャ 552
初期化
タスクマネージャ 576
(スリープ/アウェイク/コンテキストスワップ)
割込みハンドラー 584
(タイマ/BIU/電源異常/ウォッチドッグタイマ/暗号化完了)
BIU ハンドラー 586
メモリマネージャ 578
初期化(MMUテーブル設定)
割当
割当解除
仮想メモリマネージャ 580
スワップブロックページング
外部モジュールページング
メモリ圧縮
RPC およびテーブル 550
初期化
メッセージングコード/サービスマネージャ
送信/受信
ステータス
RPC ディスパッチテーブル
RPC サービステーブル
時間ベースマネージャ 554
暗号化/復号化マネージャ 556
PK
バルク
鍵およびタグマネージャ 558
EEPROM内での鍵保管
鍵ロケータ
鍵発生器
回転アルゴリズム
要約サービスマネージャ 560
イベント要約
予算要約
配布者要約サービス
チャネルサービスマネージャ 562
チャネルヘッダ
チャネル詳細
ロードモジュール実行サービス 568
認証マネージャ/安全な通信マネージャ 564
データベースマネージャ 566
管理ファイルサポート
取引およびシーケンス番号サポート
SRN/ハッシュ
DTDインタプリタ 590
ライブラリルーチン 574
I/Oコール(ストリングサーチ等)
おそらくライブラリルーチンである、雑項目
タグチェック、MD5、CRC
基本メソッドの内部LM672
計量ロードモジュール
課金ロードモジュール
予算ロードモジュール
監査ロードモジュール
読込オブジェクトロードモジュール
書込オブジェクトロードモジュール
オープンオブジェクトロードモジュール
クローズオブジェクトロードモジュール
SPU ROM/EEPROM/フラッシュ 532

FIG. 14A

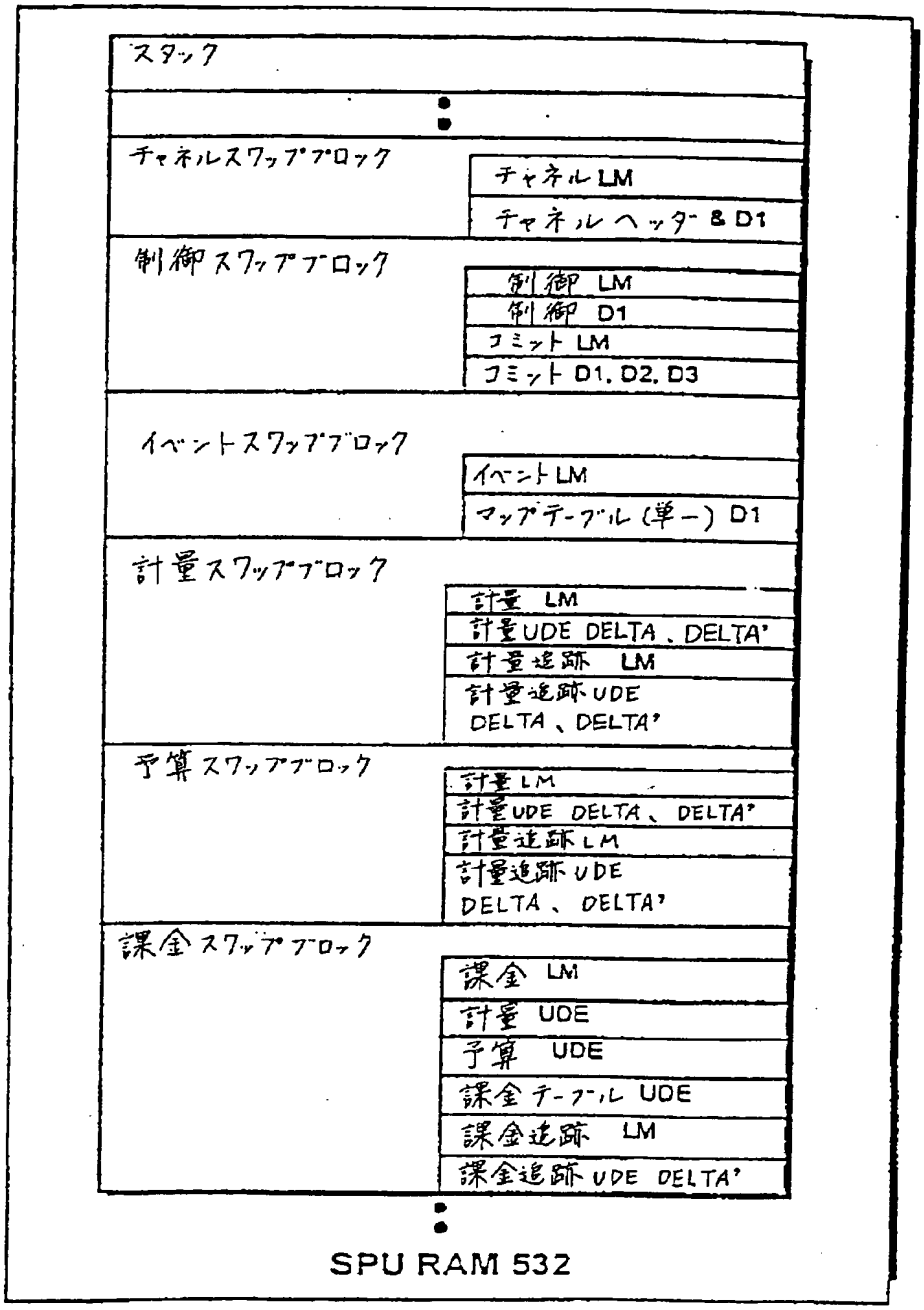
【図１４】

FIG. 14B


公開鍵および秘密鍵、システムID、認証証明書、
VDEシステム公開鍵、秘密DES鍵
オブジェクトのトップレベル鍵
トップレベル予算情報
計量加算値
予算レコードの鍵レコード、監査レコード、静的管理レコード、
更新管理レコード、等
デバイスデータテーブル
サイトID
時刻
アラーム
取引/シーケンス番号 #5
雑
メモリマップ
マップ計量
LM/UDTテーブル
タスクマネージャ 576
チャネル
要約サービス 560
安全なデータベースタグ
SRNエントリ
ハッシュエントリ
不揮発性メモリ 534b

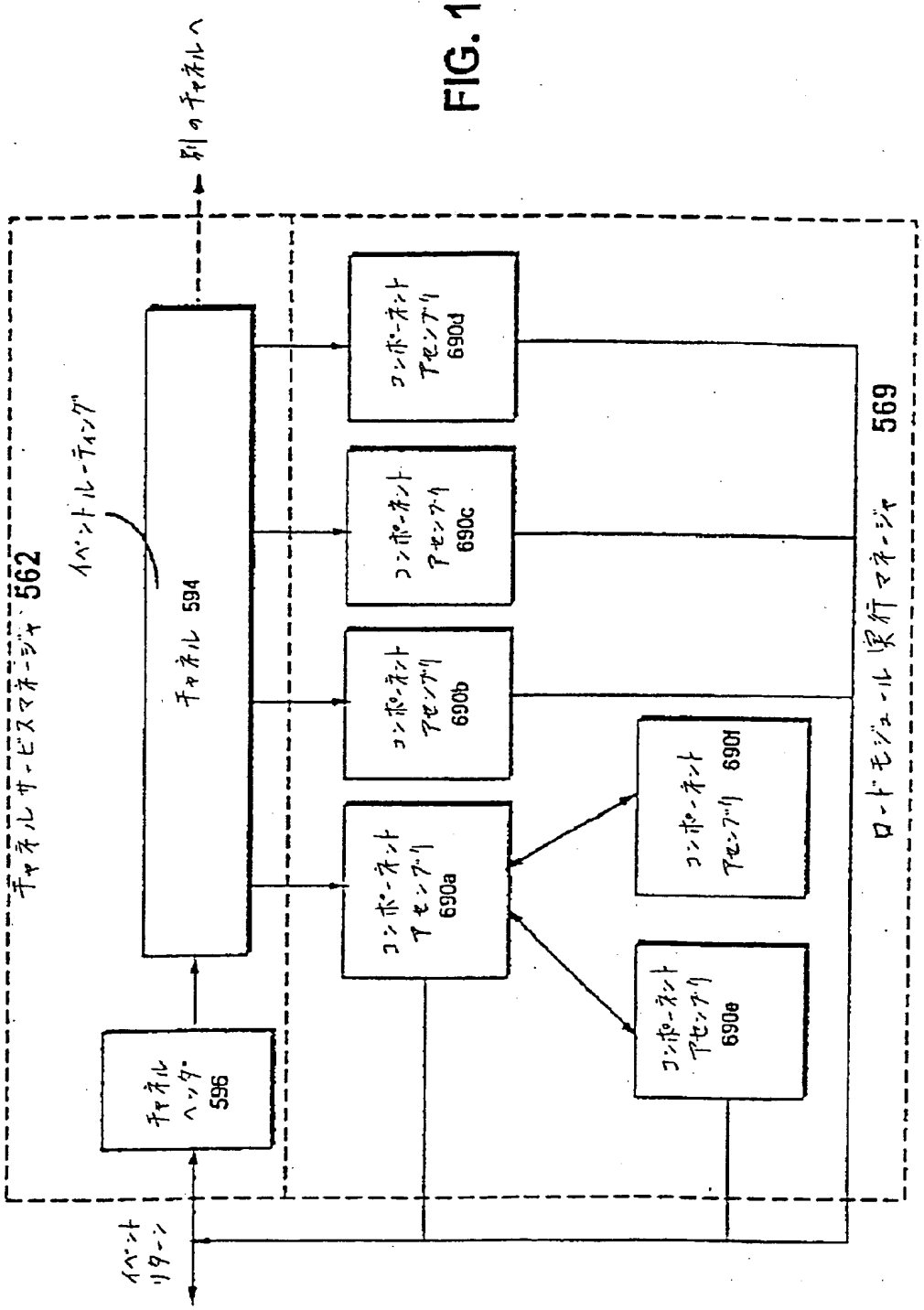
【図１４】

FIG. 14C


スタック
チャネルスワップブロック
チャネルLM
チャネルヘッダ & D1
制御スワップブロック
制御 LM
制御 D1
コミット LM
コミット D1, D2, D3
イベントスワップブロック
イベントLM
マップテーブル(単一) D1
計量スワップブロック
計量 LM
計量UDE DELTA、DELTA'
計量追跡 LM
計量追跡UDE
DELTA、DELTA'
予算スワップブロック
計量LM
計量UDE DELTA、DELTA'
計量追跡LM
計量追跡UDE
DELTA、DELTA'
課金スワップブロック
課金 LM
計量 UDE
予算 UDE
課金テーブル UDE
課金追跡 LM
課金追跡 UDE DELTA'
SPU RAM 532

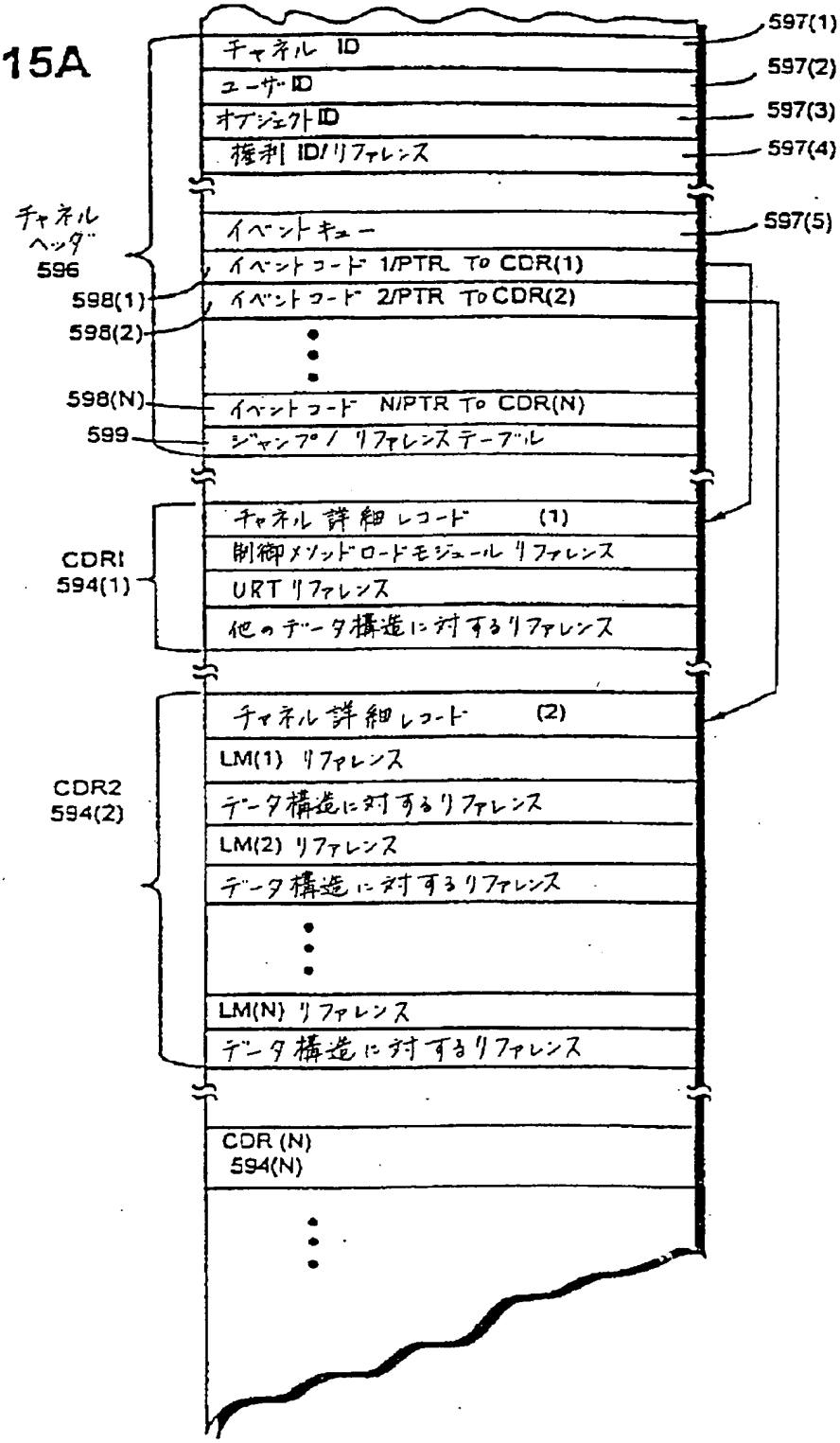
【図１５】

FIG. 15


別のチャネルへ
チャネルサービスマネージャ 562
イベントルーティング
チャネル 594
チャネル ヘッダー 596
コンポーネント アセンブリ 690a
コンポーネント アセンブリ 690b
コンポーネント アセンブリ 690c
コンポーネント アセンブリ 690d
コンポーネント アセンブリ 690e
コンポーネント アセンブリ 690f
ロードモジュール実行マネージャ 569
イベント リターン

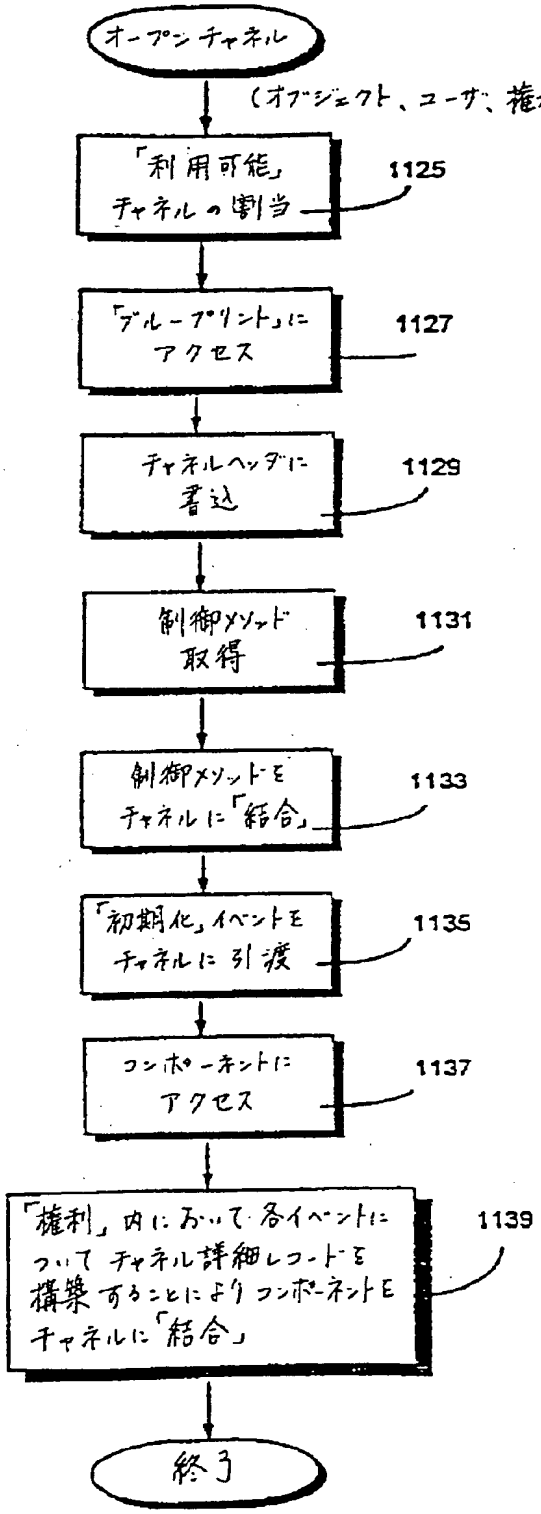
【図１５】

FIG. 15A


チャネル ID
ユーザID
オブジェクトID
権利 ID/リファレンス
597(1)
597(2)
597(3)
597(4)
チャネル ヘッダ 596
イベントキュー
597(5)
イベントコード 1/PTR To CDR(1)
598(1)
イベントコード 2/PTR To CDR(2)
598(2)
598(N)
イベントコード N/PTR To CDR(N)
599
ジャンプ/リファレンステーブル
CDR1 594(1)
チャネル詳細レコード (1)
制御メソッドロードモジュールリファレンス
URTリファレンス
他のデータ構造に対するリファレンス
CDR2 594(2)
チャネル詳細レコード (2)
LM(1) リファレンス
データ構造に対するリファレンス
LM(2) リファレンス
データ構造に対するリファレンス
LM(N) リファレンス
データ構造に対するリファレンス
CDR (N) 594(N)

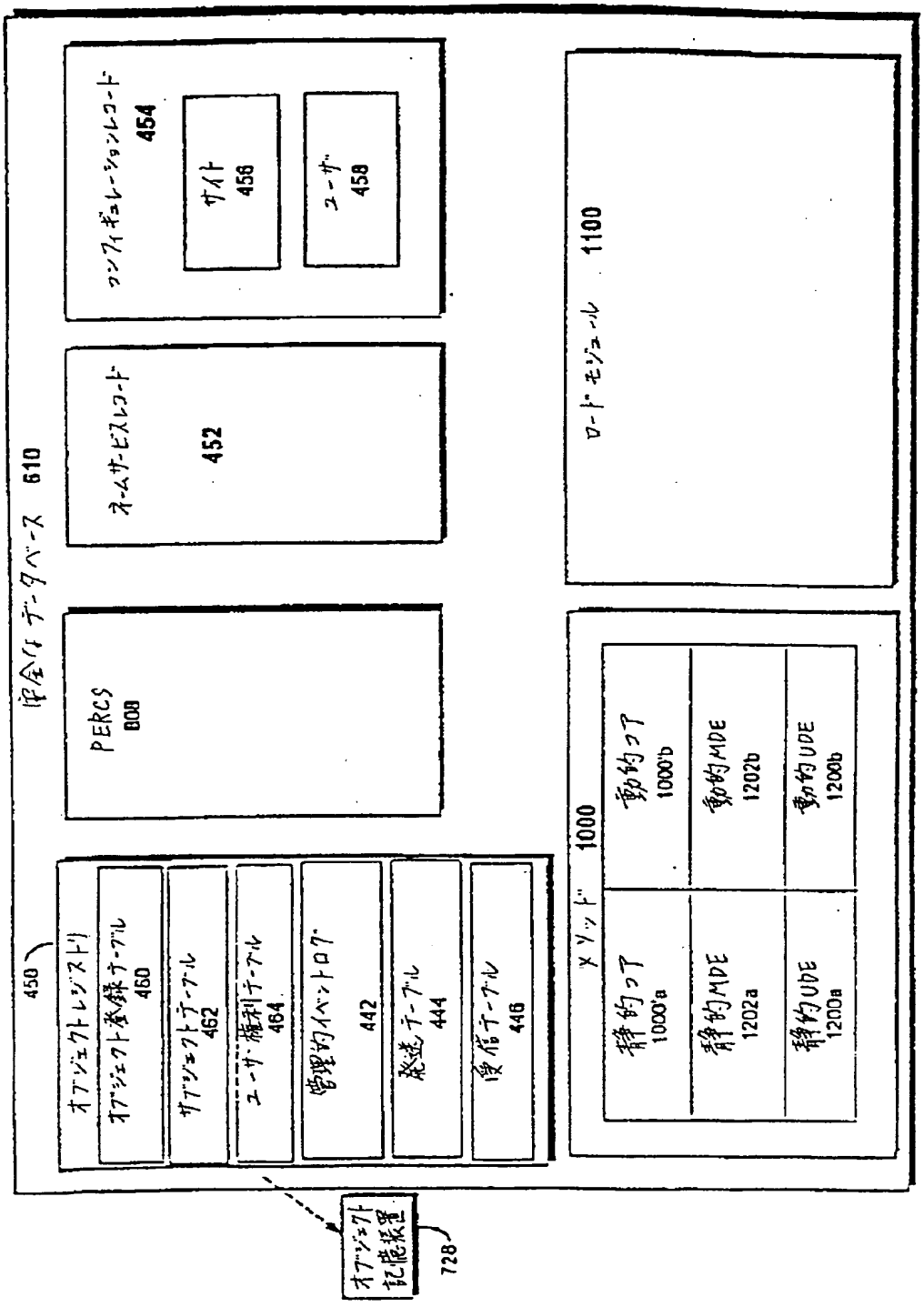
【図１５】

FIG. 15B


オープンチャネル
（オブジェクト、ユーザ、権利）
「利用可能」チャネルの割当
1125
「ブループリント」にアクセス
1127
チャネルヘッダに書込
1129
制御メソッド取得
1131
制御メソッドをチャネルに「結合」
1133
「初期化」イベントをチャネルに引渡
1135
コンポーネントにアクセス
1137
「権利」内において各イベントについてチャネル詳細レコードを構築することによりコンポーネントをチャネルに「結合」
1139
終了

【図16】

FIG. 16


安全なデータベース 610
450
オブジェクトレジストリ
オブジェクト登録テーブル 460
サブジェクトテーブル 462
ユーザ権利テーブル 464
管理的イベントログ 442
発送テーブル 444
受信テーブル 446
PERCS 800
ネームサービスレコード 452
コンフィギュレーションレコード 454
サイト 456
ユーザ 458
ロードモジュール 1100
メソッド 1000
静的コア 1000a
動的コア 1000b
静的MDE 1202a
動的MDE 1202b
静的UDE 1200a
動的UDE 1200b
オブジェクト記憶装置 728

【図１７】

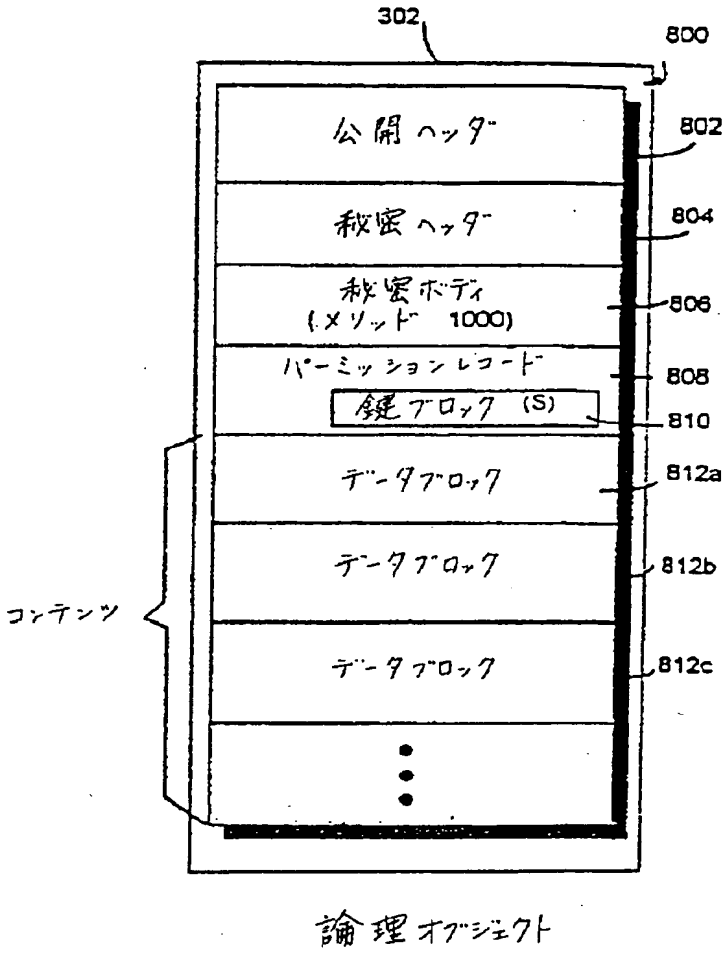
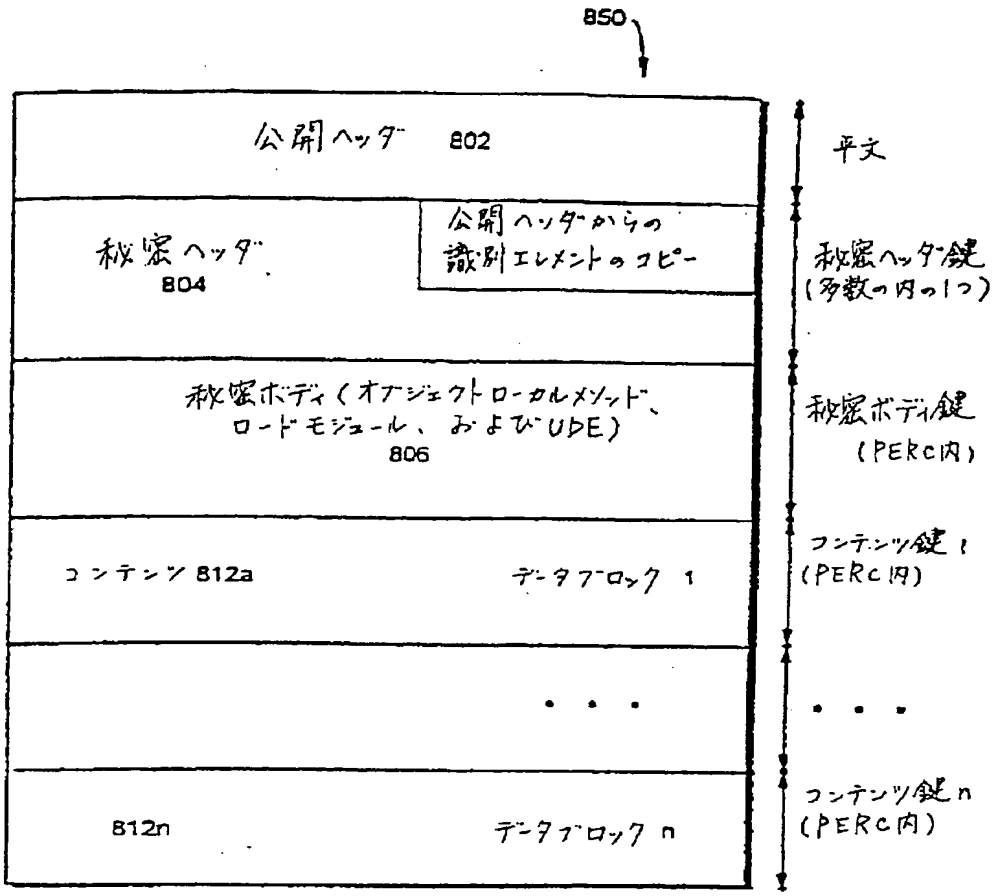

302
800
公開ヘッダ
802
秘密ヘッダ
804
秘密ボディ
(メソッド 1000)
806
パーミッションレコード
808
鍵ブロック (S)
810
データブロック
812a
データブロック
812b
データブロック
812c
コンテンツ
論理オブジェクト

FIG. 17

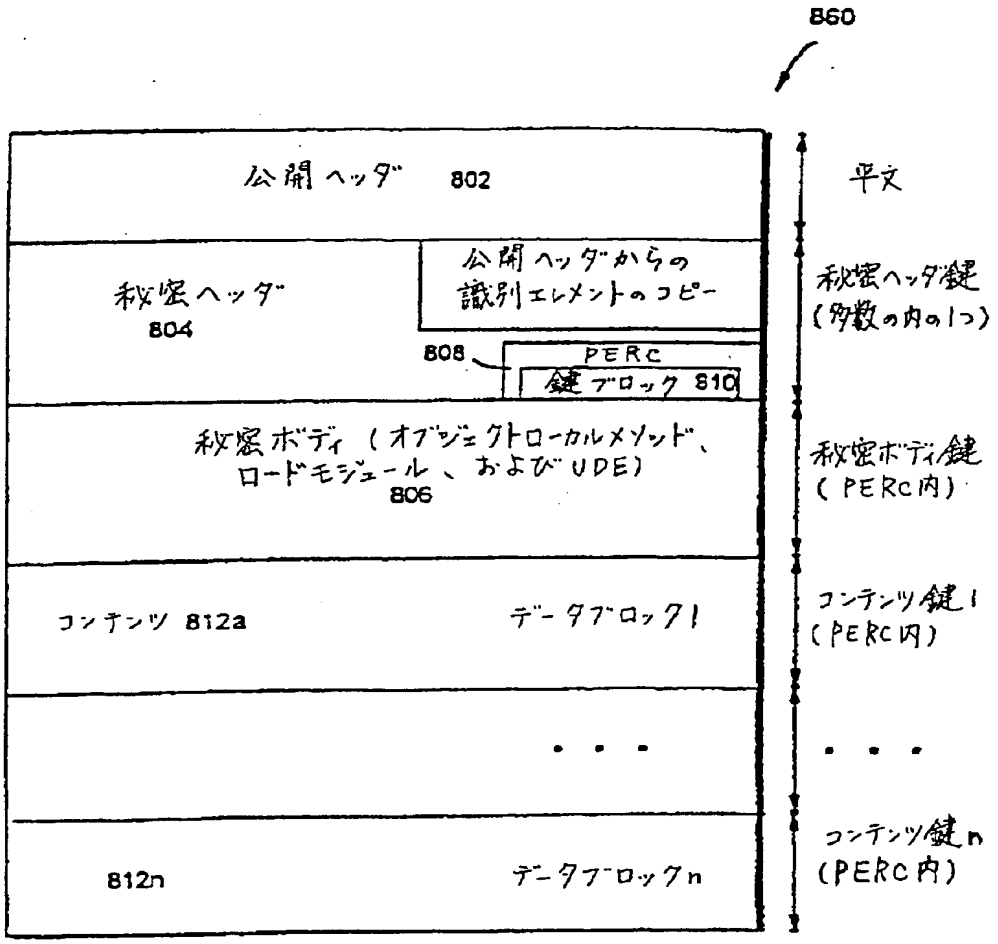
【図１８】



静止オブジェクト

FIG. 18

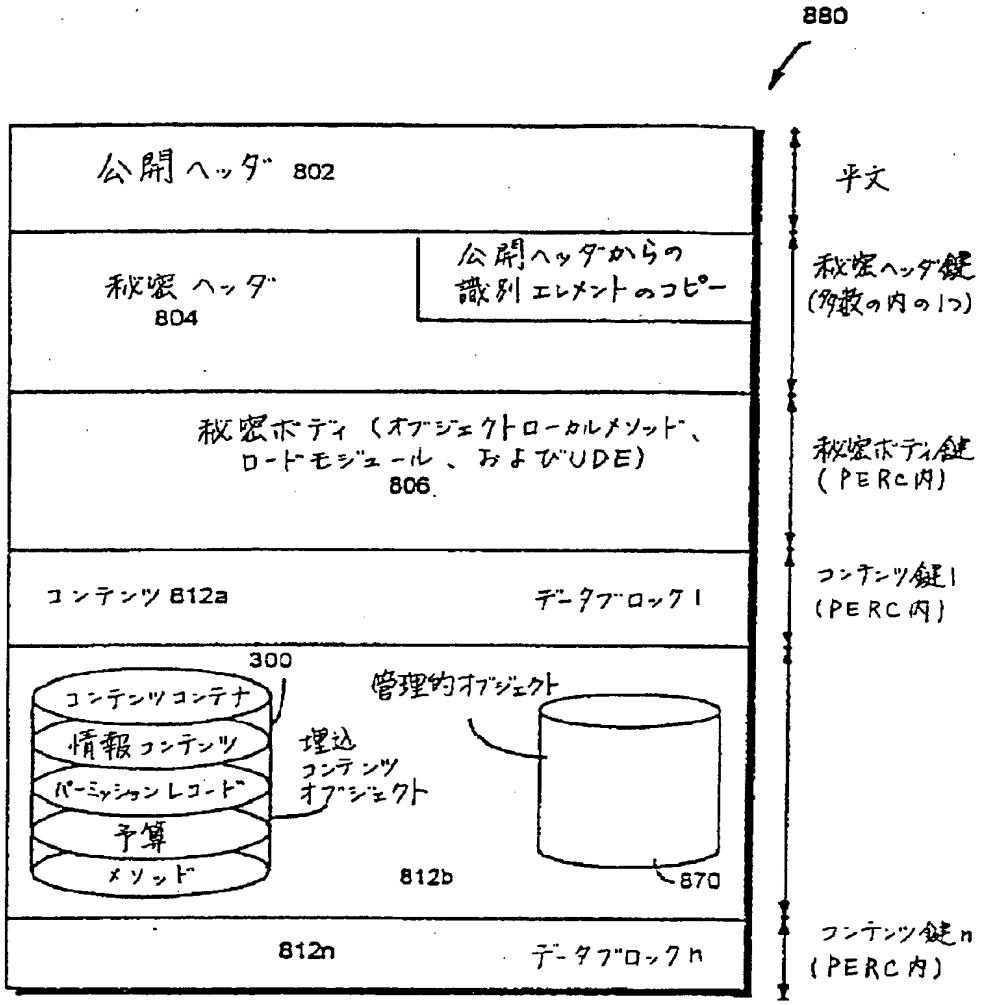
【図１９】



移動オブジェクト

FIG. 19

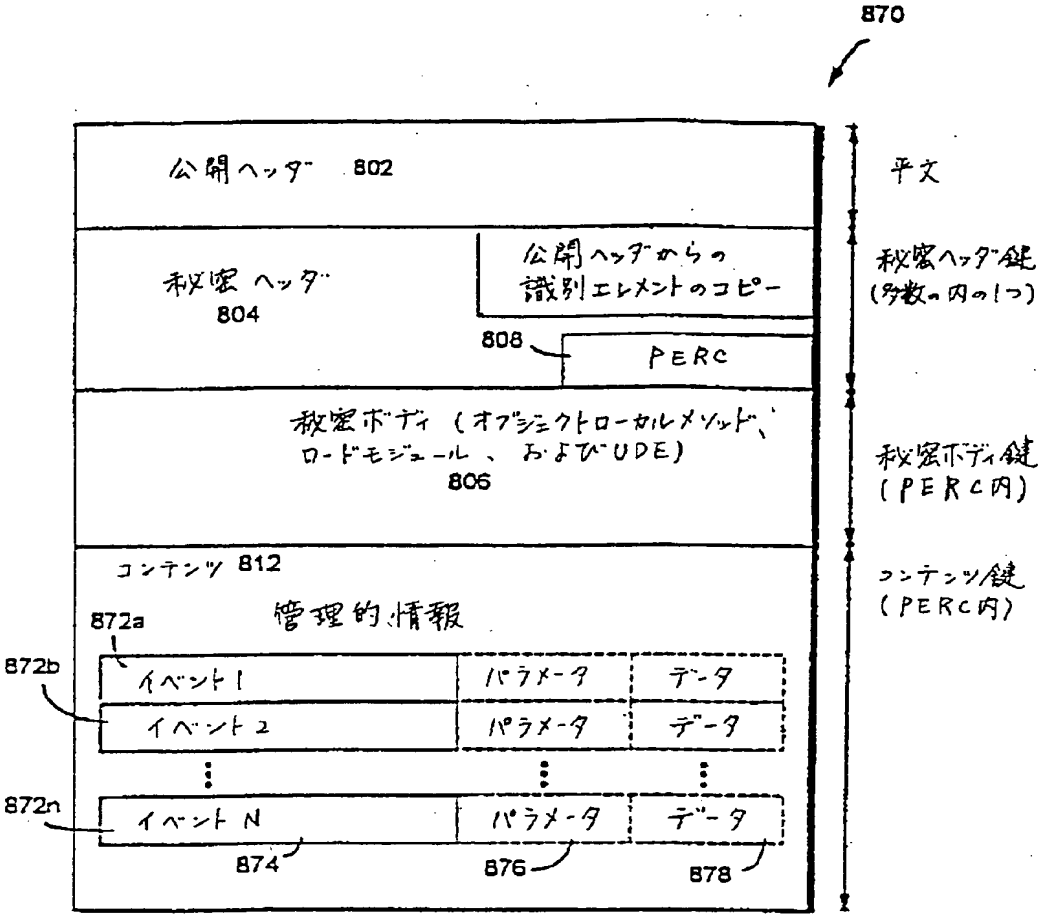
【図２０】



コンテンツ オブジェクト

FIG. 20

【図２１】

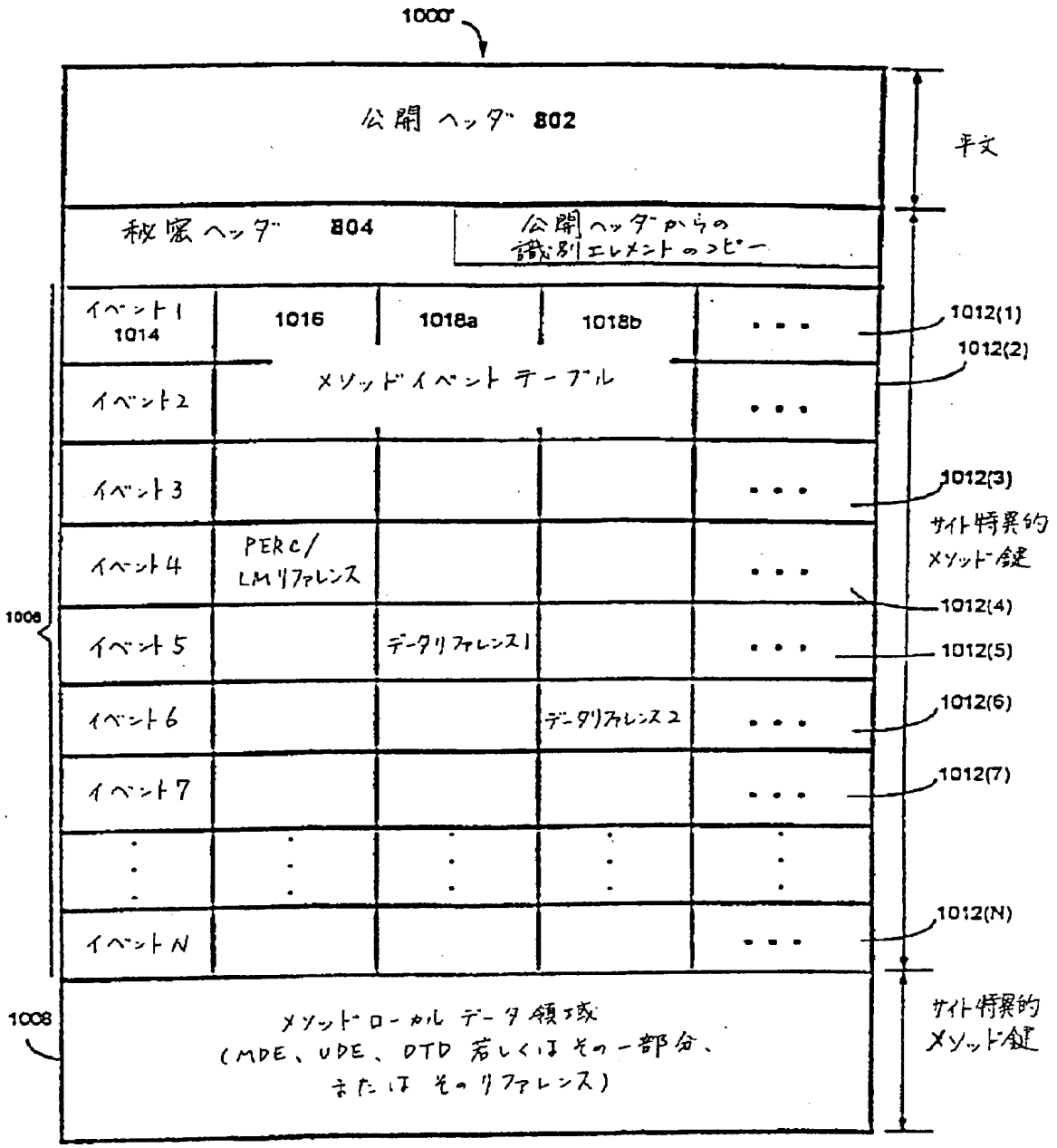


管理的オブジェクト

FIG. 21

【図２２】

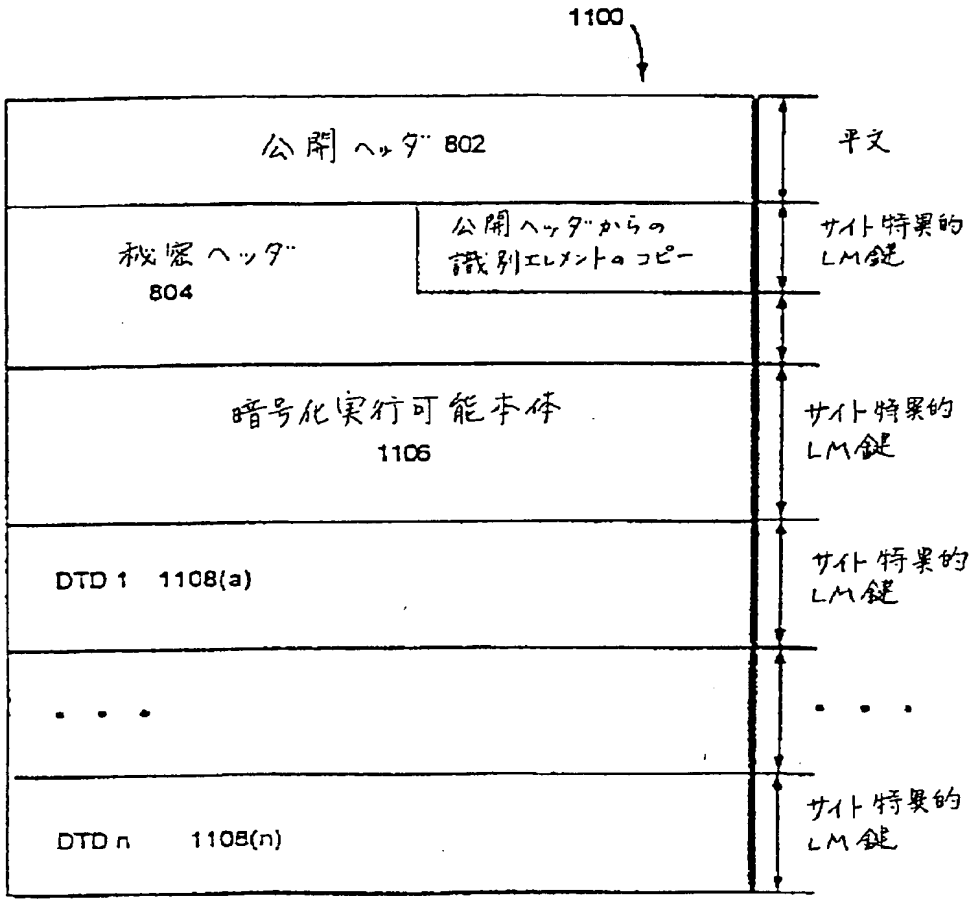
FIG. 22



メソッド「コア」

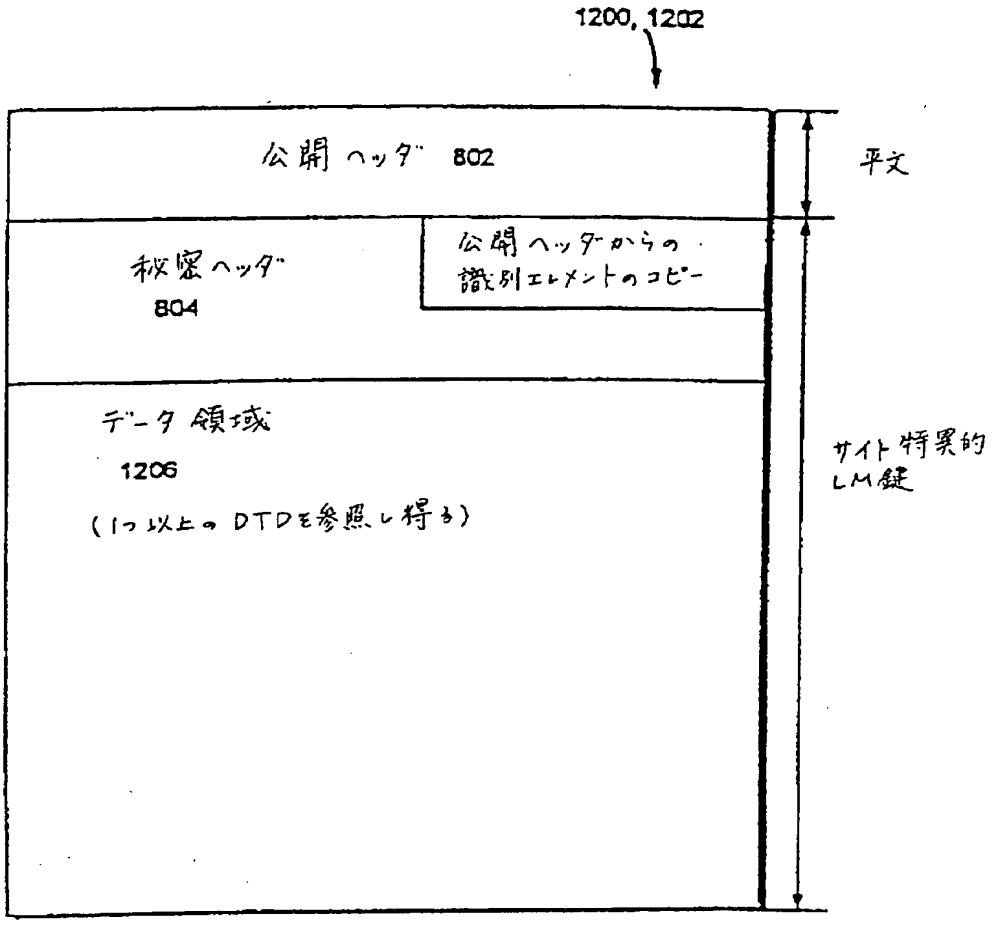
【図２３】

FIG. 23


1100
公開ヘッダ 802
平文
秘密ヘッダ
804
公開ヘッダからの
識別エレメントのコピー
サイト特異的
LM鍵
暗号化実行可能本体
1106
サイト特異的
LM鍵
DTD 1　1108(a)
サイト特異的
LM鍵
・ ・ ・
・ ・ ・
DTD n　1108(n)
サイト特異的
LM鍵

【図２４】

FIG. 24



UDE (MDE)

【図２５】

FIG. 25A

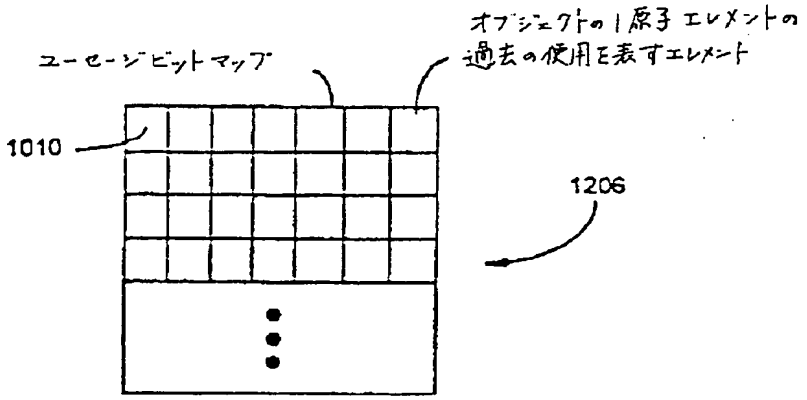
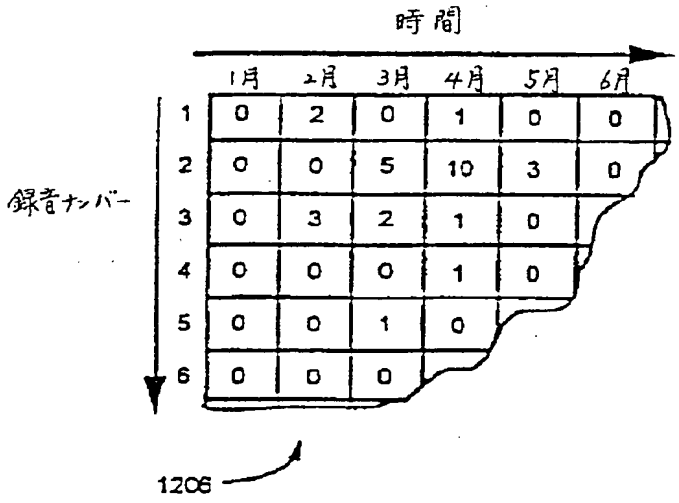
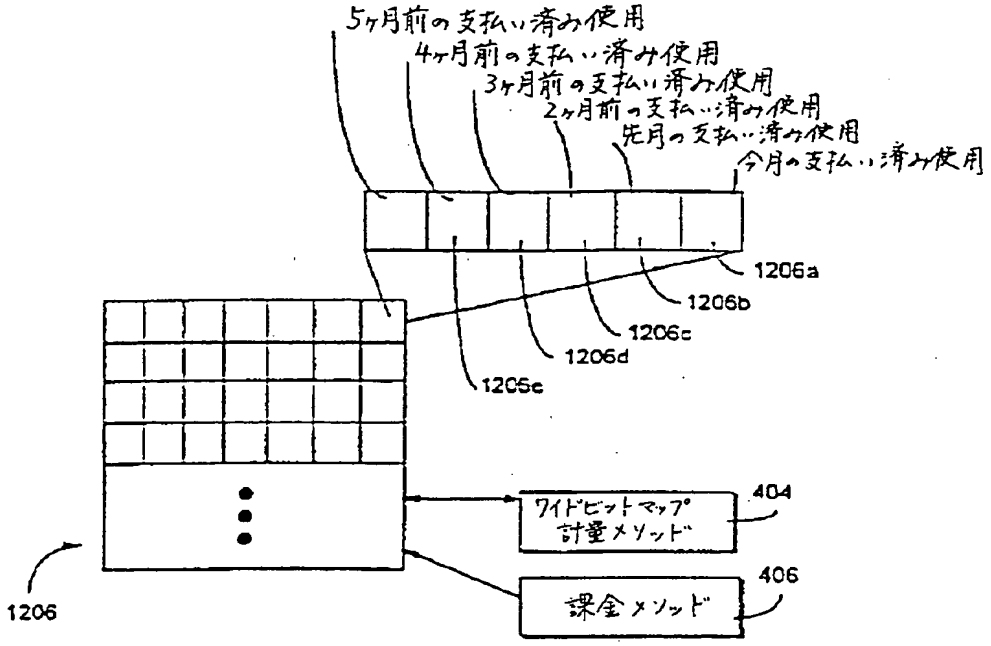


FIG. 25B



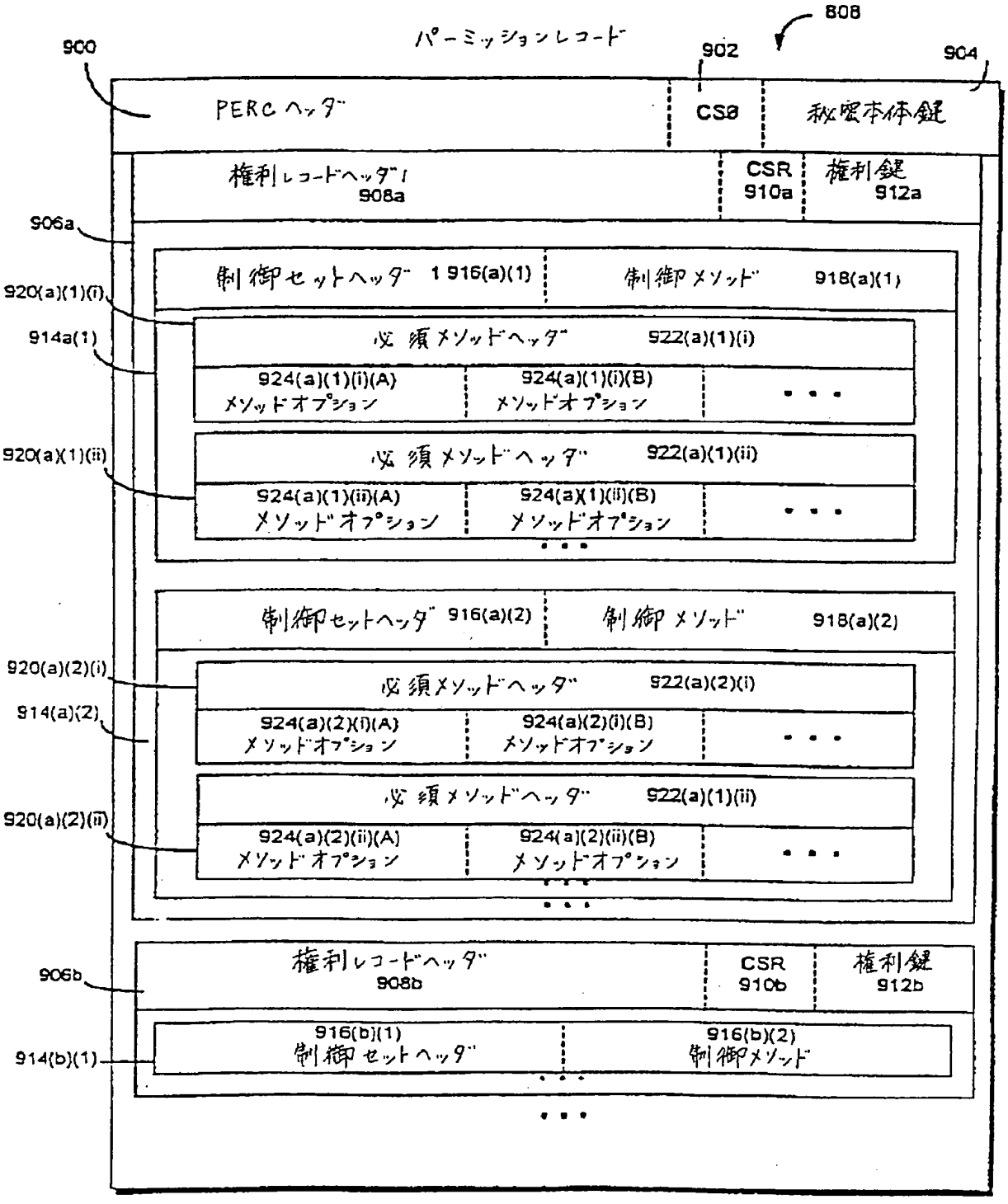
【図２５】

FIG. 25C


5ヶ月前の支払い済み使用
4ヶ月前の支払い済み使用
3ヶ月前の支払い済み使用
2ヶ月前の支払い済み使用
先月の支払い済み使用
今月の支払い済み使用
1206a
1206b
1206c
1206d
1206e
ワイドビットマップ
計量メソッド
404
課金メソッド
406
1206

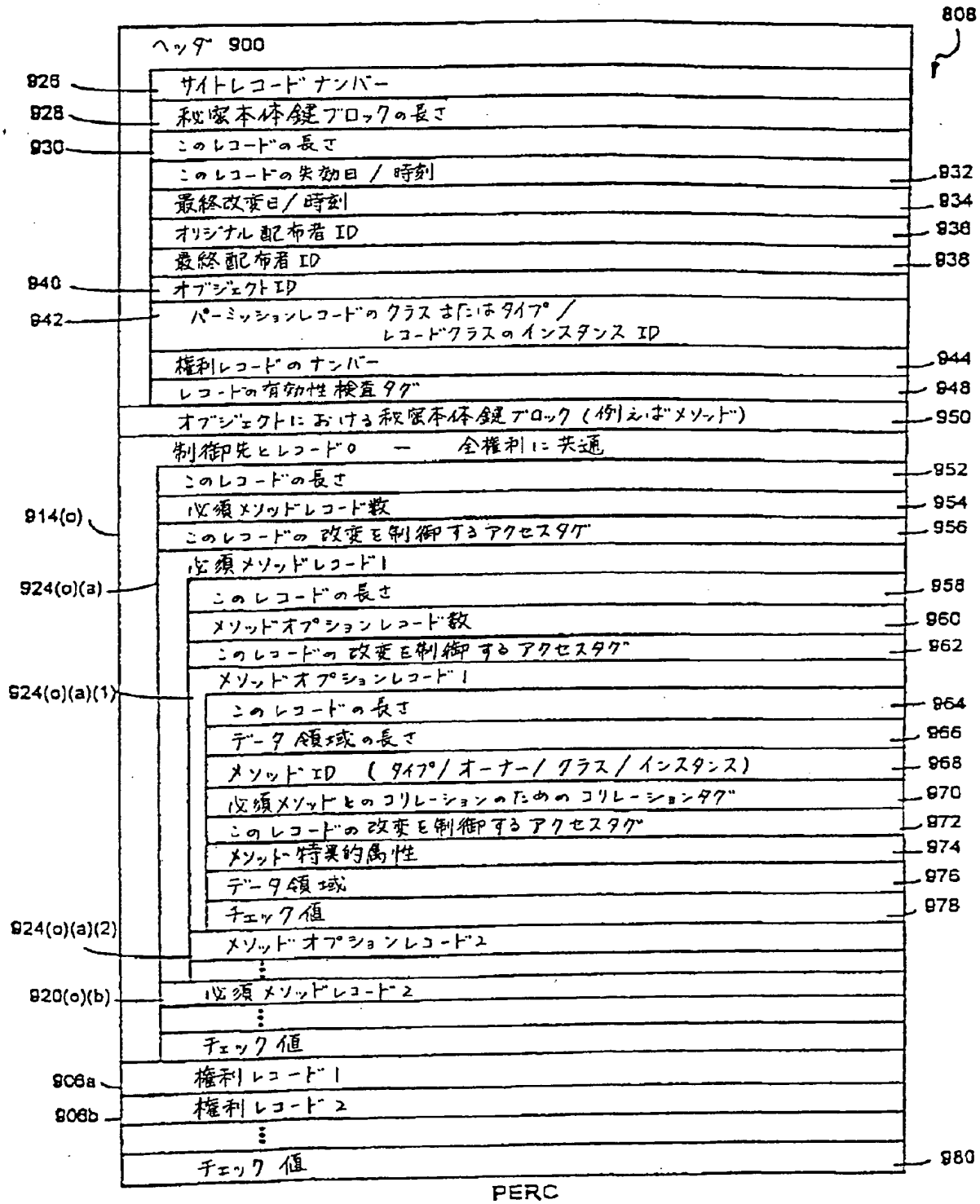
【図２６】

FIG. 26


808
パーミッションレコード
900
902
904
PERC ヘッダ
CS8
秘密本体鍵
権利レコードヘッダ1
908a
CSR
910a
権利鍵
912a
906a
制御セットヘッダ 1 916(a)(1)
制御メソッド 918(a)(1)
920(a)(1)(i)
914a(1)
必須メソッドヘッダ 922(a)(1)(i)
924(a)(1)(i)(A)
メソッドオプション
924(a)(1)(i)(B)
メソッドオプション
920(a)(1)(ii)
必須メソッドヘッダ 922(a)(1)(ii)
924(a)(1)(ii)(A)
メソッドオプション
924(a)(1)(ii)(B)
メソッドオプション
制御セットヘッダ 916(a)(2)
制御メソッド 918(a)(2)
920(a)(2)(i)
914(a)(2)
必須メソッドヘッダ 922(a)(2)(i)
924(a)(2)(i)(A)
メソッドオプション
924(a)(2)(i)(B)
メソッドオプション
920(a)(2)(ii)
必須メソッドヘッダ 922(a)(1)(ii)
924(a)(2)(ii)(A)
メソッドオプション
924(a)(2)(ii)(B)
メソッドオプション
906b
権利レコードヘッダ
908b
CSR
910b
権利鍵
912b
914(b)(1)
916(b)(1)
制御セットヘッダ
916(b)(2)
制御メソッド

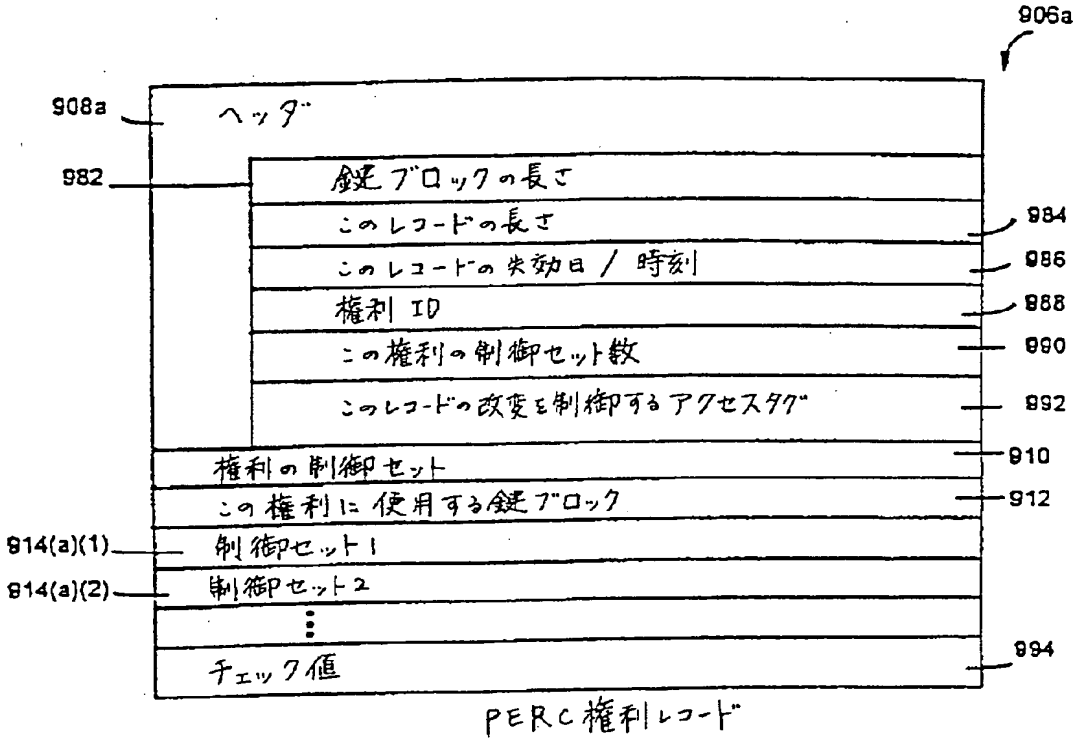
【図２６】

FIG. 26A


808
ヘッダ 900
926
サイトレコードナンバー
928
秘密本体鍵ブロックの長さ
930
このレコードの長さ
このレコードの失効日／時刻
932
最終改変日／時刻
934
オリジナル配布者 ID
936
最終配布者 ID
938
940
オブジェクト ID
942
パーミッションレコードのクラスまたはタイプ／
レコードクラスのインスタンス ID
権利レコードのナンバー
944
レコードの有効性検査タグ
948
オブジェクトにおける秘密本体鍵ブロック（例えばメソッド）
950
制御先レコード0 ― 全権利に共通
このレコードの長さ
952
必須メソッドレコード数
954
914(o)
このレコードの改変を制御するアクセスタグ
956
必須メソッドレコード1
924(o)(a)
このレコードの長さ
958
メソッドオプションレコード数
960
このレコードの改変を制御するアクセスタグ
962
メソッドオプションレコード1
924(o)(a)(1)
このレコードの長さ
964
データ領域の長さ
966
メソッド ID （タイプ／オーナー／クラス／インスタンス）
968
必須メソッドとのコリレーションのためのコリレーションタグ
970
このレコードの改変を制御するアクセスタグ
972
メソッド特異的属性
974
データ領域
976
チェック値
978
924(o)(a)(2)
メソッドオプションレコード2
920(o)(b)
必須メソッドレコード2
チェック値
906a
権利レコード1
906b
権利レコード2
チェック値
980
PERC

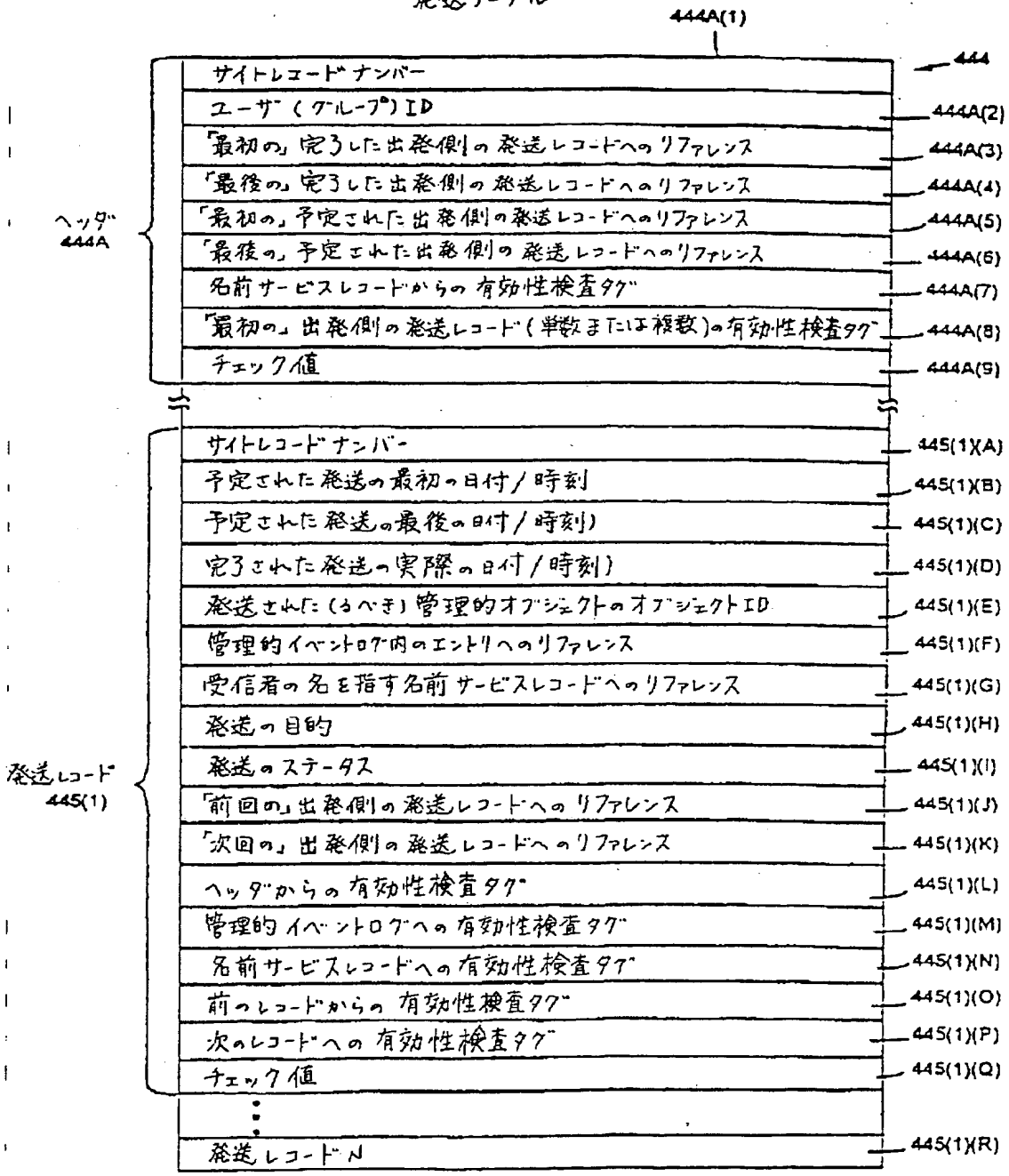
【図２６】

FIG. 26B


906a
908a
ヘッダ
982
鍵ブロックの長さ
このレコードの長さ
984
このレコードの失効日 / 時刻
986
権利 ID
988
この権利の制御セット数
990
このレコードの改変を制御するアクセスタグ
992
権利の制御セット
910
この権利に使用する鍵ブロック
912
914(a)(1)
制御セット1
914(a)(2)
制御セット2
チェック値
994
PERC権利レコード

【図27】

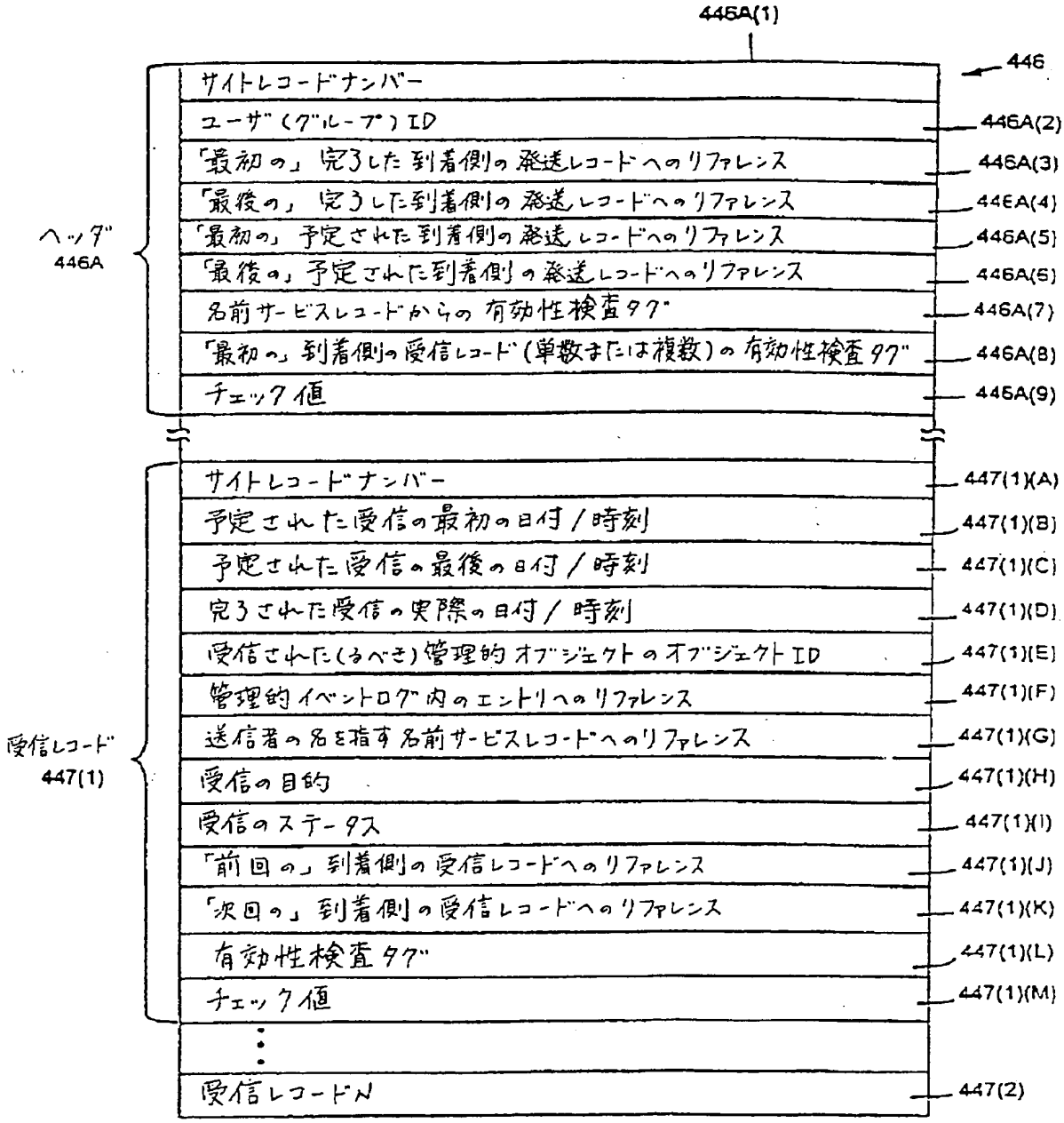
FIG. 27
発送テーブル



【図28】

FIG. 28

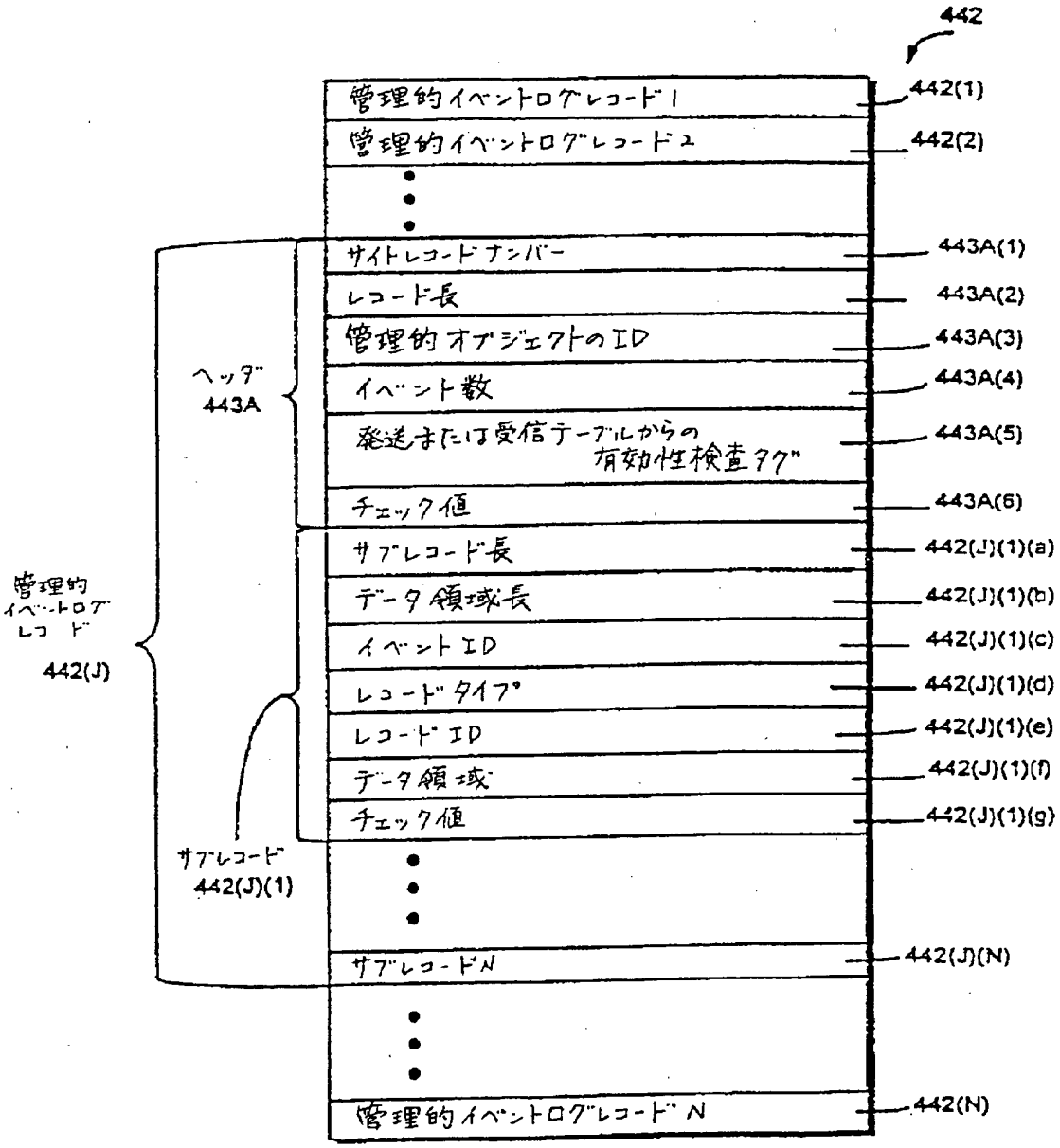
受信テーブル



【図２９】

FIG. 29

管理的イベントログ



【図30】

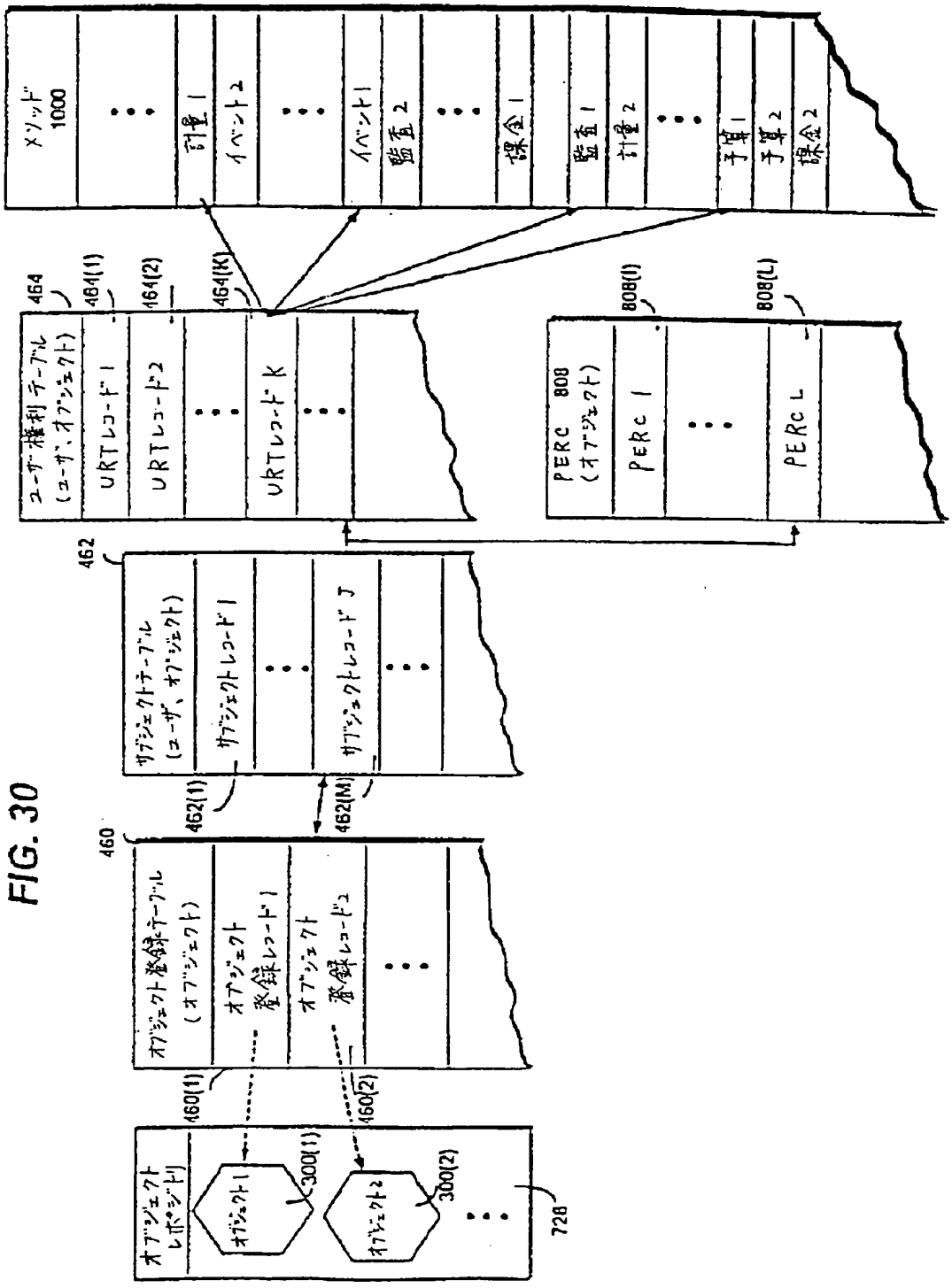

メソッド 1000
計量1
イベント2
イベント1
監査2
課金1
監査1
計量2
手算1
手算2
課金2
ユーザ権利テーブル (ユーザ、オブジェクト)
464
URTレコード1
URTレコード2
URTレコード K
464(1)
464(2)
464(K)
PERC 808 (オブジェクト)
PERC 1
PERC L
808(1)
808(L)
サブジェクトテーブル (ユーザ、オブジェクト)
462
サブジェクトレコード1
サブジェクトレコード J
462(1)
462(M)
オブジェクト登録テーブル (オブジェクト)
460
オブジェクト登録レコード1
オブジェクト登録レコード2
160(1)
160(2)
オブジェクト レポジトリ
オブジェクト1
オブジェクト2
300(1)
300(2)
728

FIG. 30

【図３１】

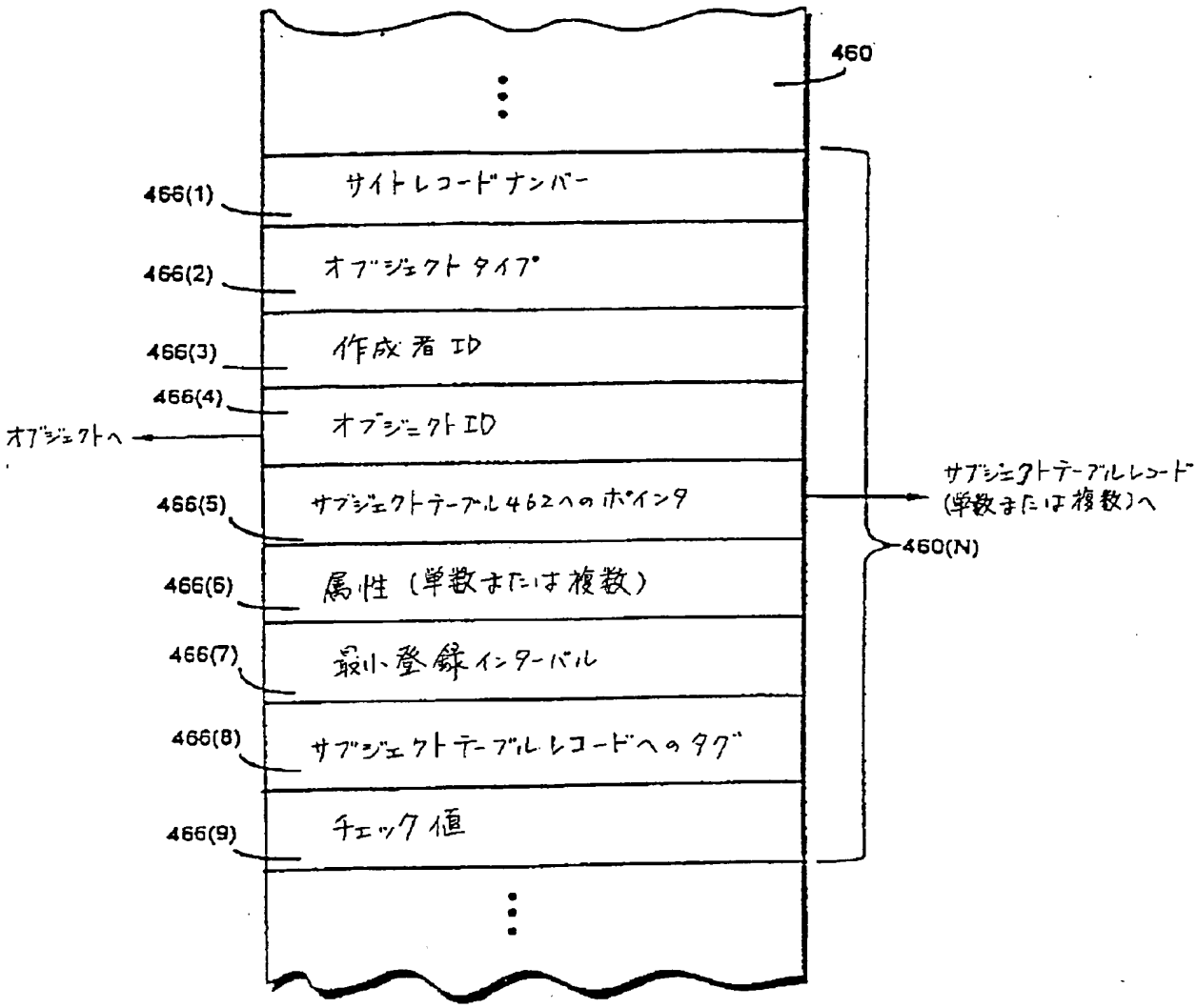
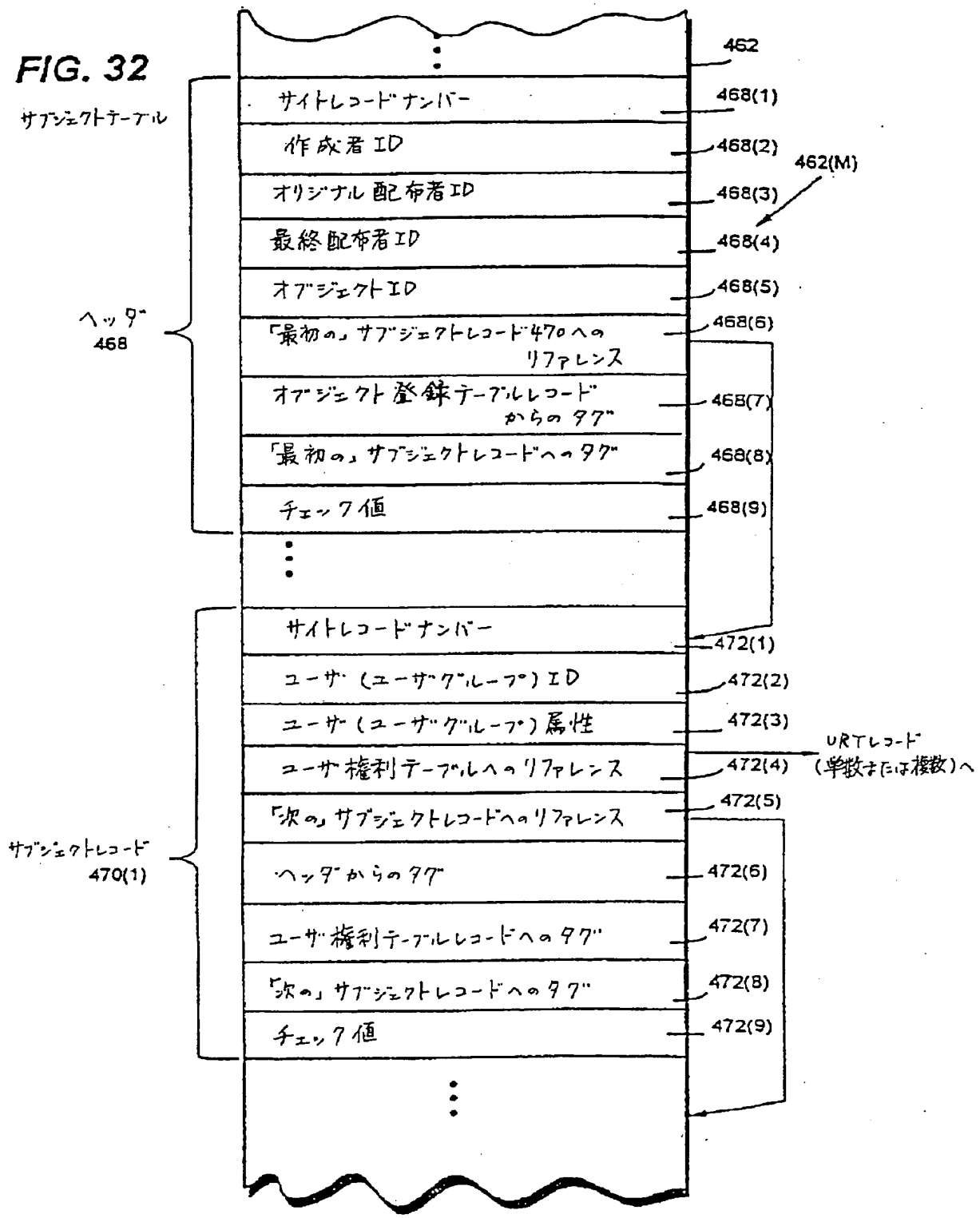


FIG. 31
オブジェクト登録テーブル

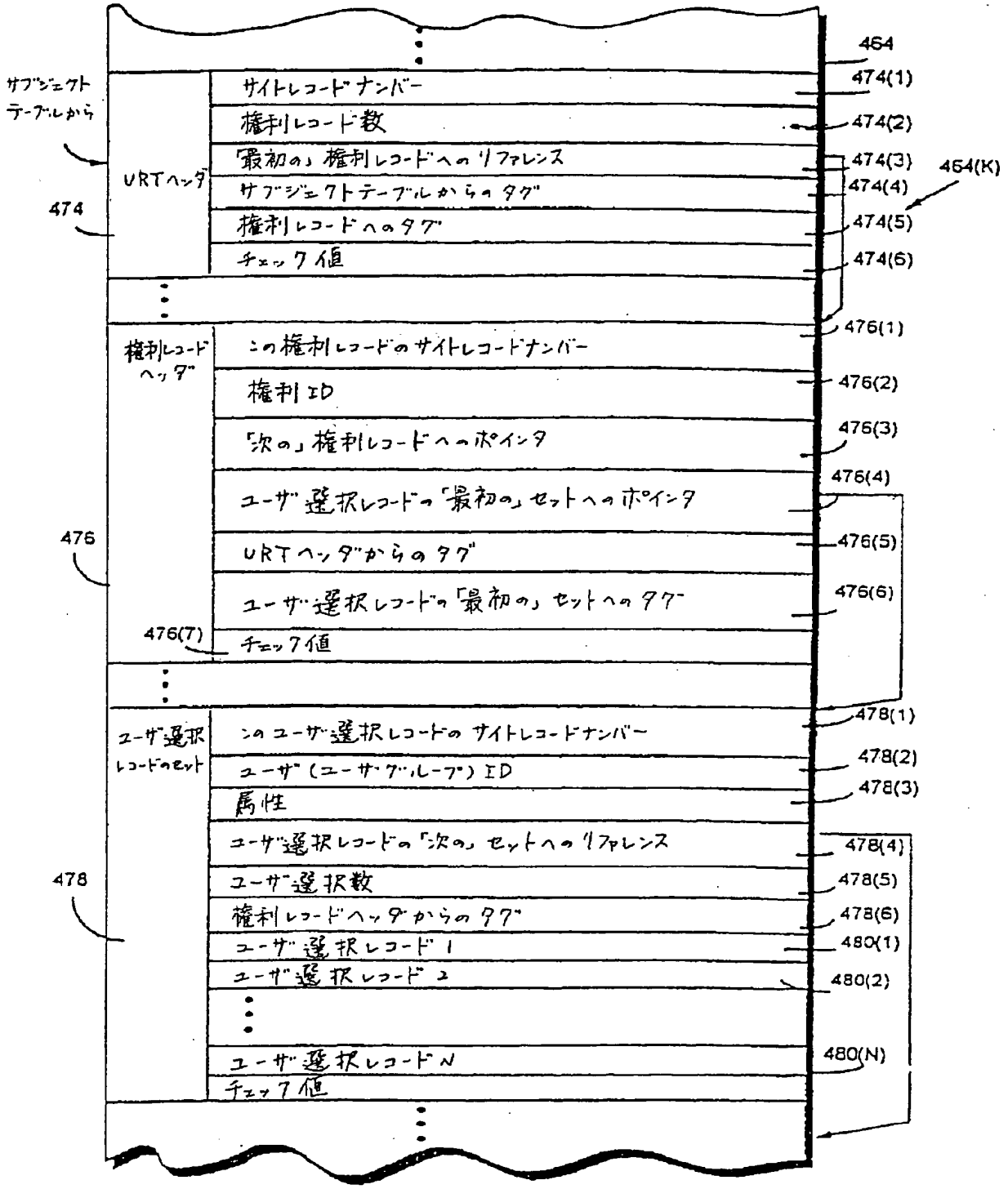
【図32】

FIG. 32


サブジェクトテーブル
462
サイトレコードナンバー
468(1)
作成者ID
468(2)
462(M)
オリジナル配布者ID
468(3)
最終配布者ID
468(4)
オブジェクトID
468(5)
ヘッダ
468
「最初の」サブジェクトレコード470へのリファレンス
468(6)
オブジェクト登録テーブルレコードからのタグ
468(7)
「最初の」サブジェクトレコードへのタグ
468(8)
チェック値
468(9)
サイトレコードナンバー
472(1)
ユーザ(ユーザグループ)ID
472(2)
ユーザ(ユーザグループ)属性
472(3)
URTレコード(単数または複数)へ
ユーザ権利テーブルへのリファレンス
472(4)
「次の」サブジェクトレコードへのリファレンス
472(5)
サブジェクトレコード
470(1)
ヘッダからのタグ
472(6)
ユーザ権利テーブルレコードへのタグ
472(7)
「次の」サブジェクトレコードへのタグ
472(8)
チェック値
472(9)

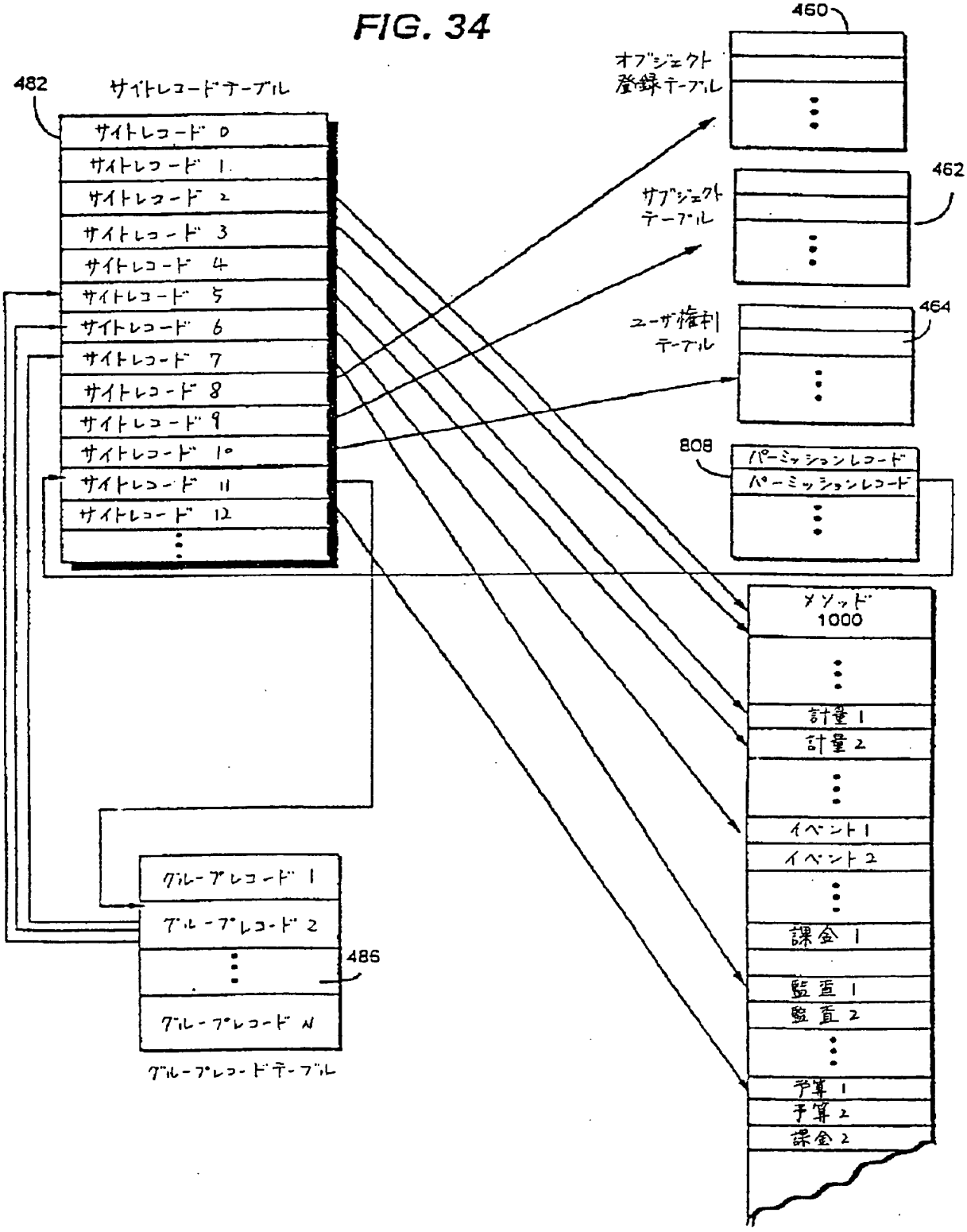
【図33】

FIG. 33　ユーザ権利テーブル



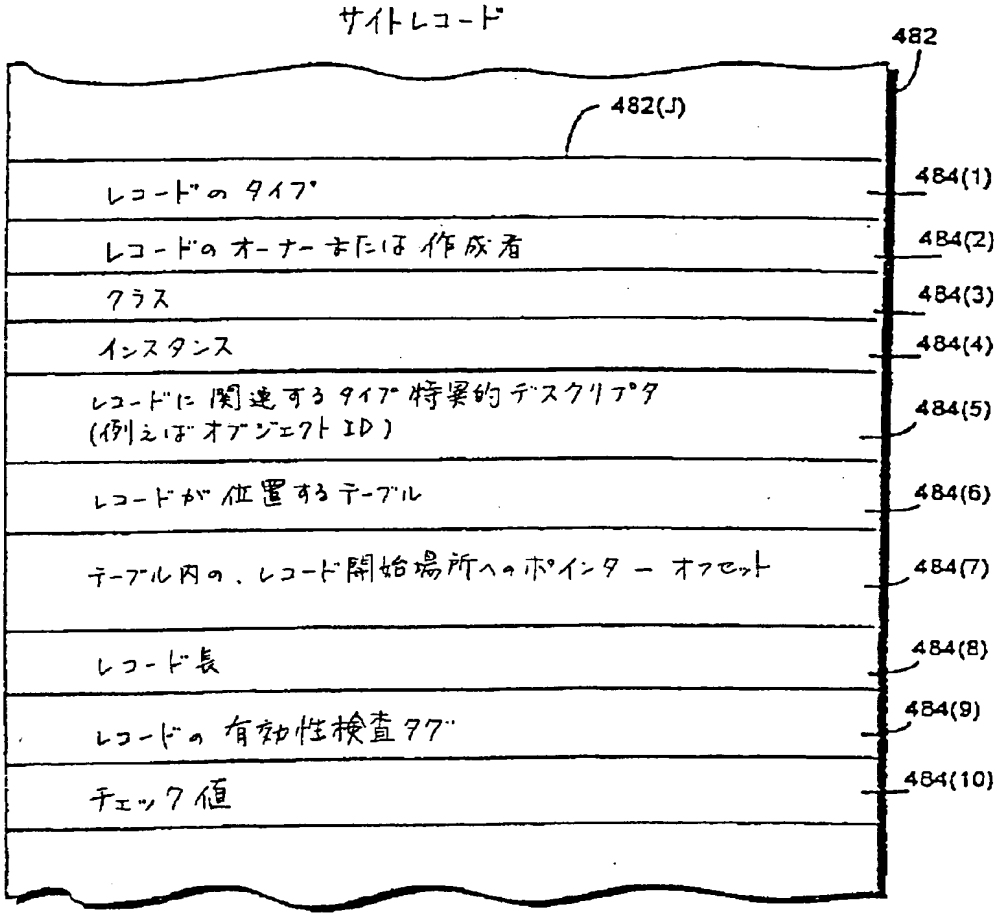
【図３４】

FIG. 34


460
オブジェクト登録テーブル
462
サブジェクトテーブル
464
ユーザ権利テーブル
808
パーミッションレコード
パーミッションレコード
482
サイトレコードテーブル
サイトレコード 0
サイトレコード 1
サイトレコード 2
サイトレコード 3
サイトレコード 4
サイトレコード 5
サイトレコード 6
サイトレコード 7
サイトレコード 8
サイトレコード 9
サイトレコード 10
サイトレコード 11
サイトレコード 12
メソッド 1000
計量 1
計量 2
イベント 1
イベント 2
課金 1
監査 1
監査 2
予算 1
予算 2
課金 2
グループレコード 1
グループレコード 2
グループレコード N
486
グループレコードテーブル

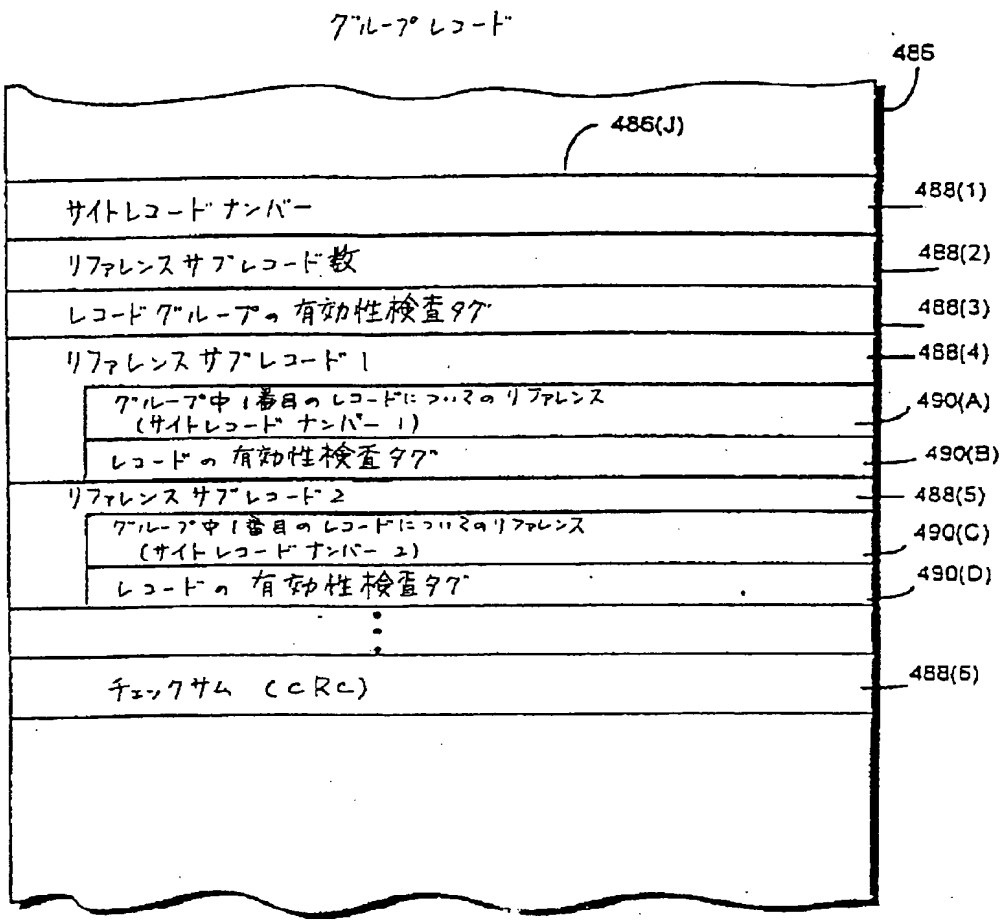
【図３４】

FIG. 34A


サイトレコード
482
482(J)
レコードのタイプ
484(1)
レコードのオーナーまたは作成者
484(2)
クラス
484(3)
インスタンス
484(4)
レコードに関連するタイプ特異的デスクリプタ
(例えばオブジェクトID)
484(5)
レコードが位置するテーブル
484(6)
テーブル内の、レコード開始場所へのポインター オフセット
484(7)
レコード長
484(8)
レコードの有効性検査ﾌﾗｸﾞ
484(9)
チェック値
484(10)

【図34】

FIG. 34B


グループレコード
485
486(J)
サイトレコードナンバー
488(1)
リファレンスサブレコード数
488(2)
レコードグループの有効性検査タグ
488(3)
リファレンスサブレコード1
488(4)
グループ中1番目のレコードについてのリファレンス
(サイトレコードナンバー1)
490(A)
レコードの有効性検査タグ
490(B)
リファレンスサブレコード2
488(5)
グループ中1番目のレコードについてのリファレンス
(サイトレコードナンバー2)
490(C)
レコードの有効性検査タグ
490(D)
チェックサム (CRC)
488(6)

【図３５】

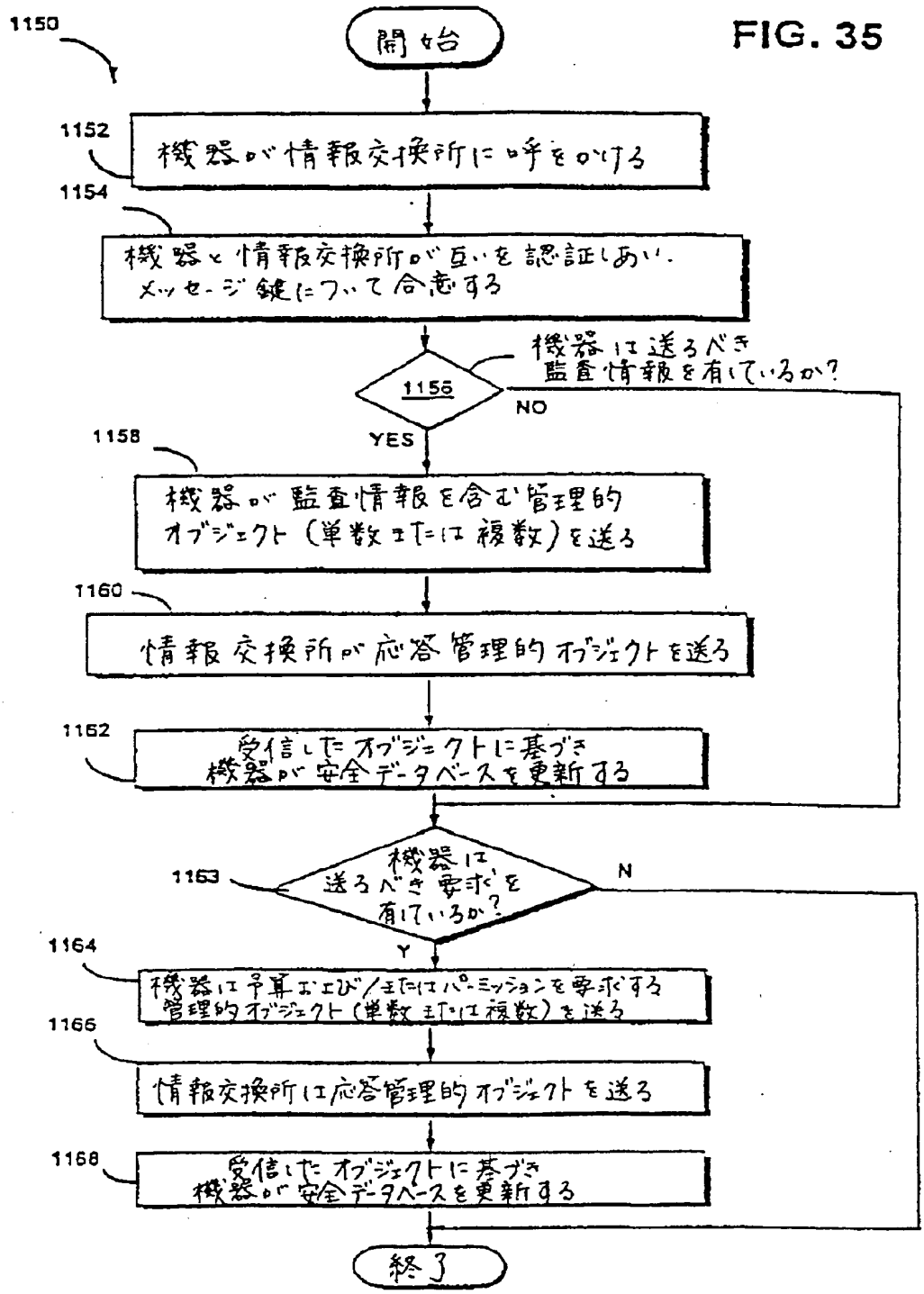
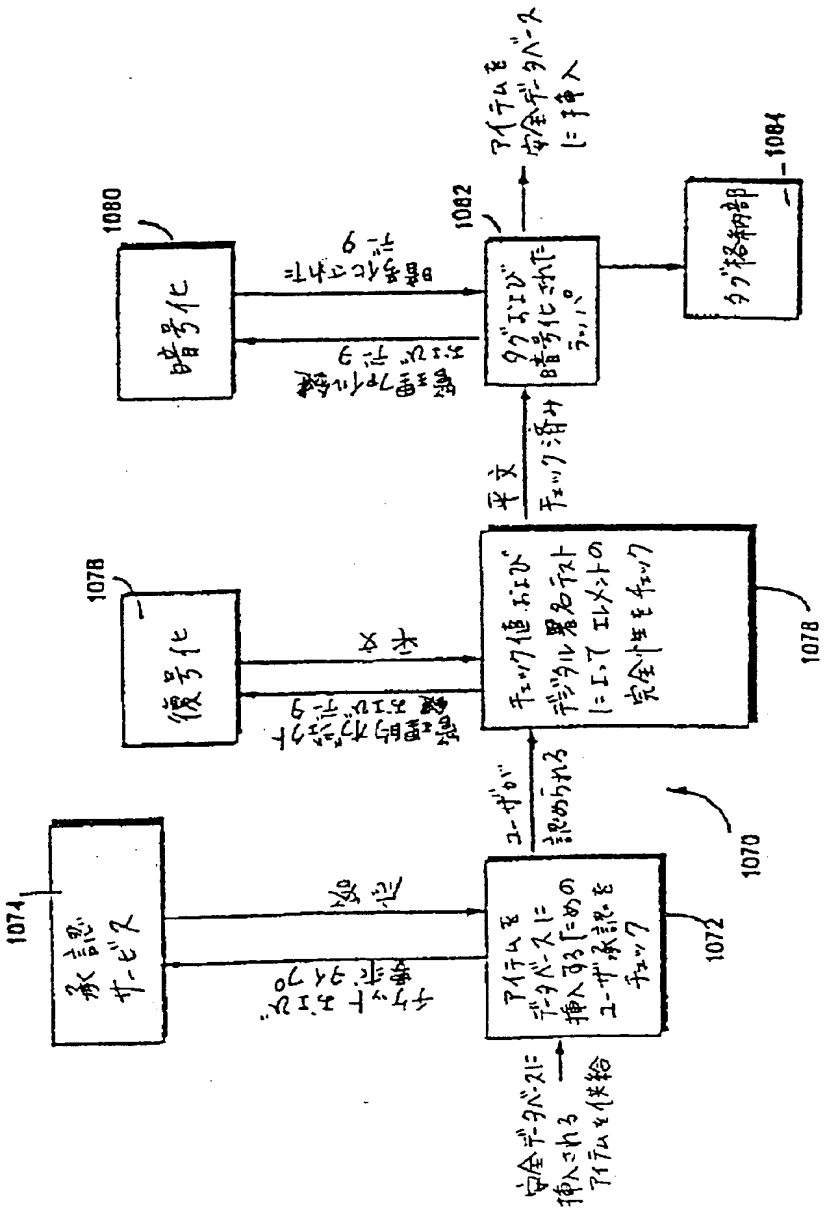

1150
開始
1152
機器が情報交換所に呼をかける
1154
機器と情報交換所が互いを認証しあい、メッセージ鍵について合意する
機器は送るべき監査情報を有しているか?
1156
NO
YES
1158
機器が監査情報を含む管理的オブジェクト（単数または複数）を送る
1160
情報交換所が応答管理的オブジェクトを送る
1162
受信したオブジェクトに基づき機器が安全データベースを更新する
機器は送るべき要求を有しているか?
1163
N
Y
1164
機器は予算および/またはパーミッションを要求する管理的オブジェクト（単数または複数）を送る
1166
情報交換所は応答管理的オブジェクトを送る
1168
受信したオブジェクトに基づき機器が安全データベースを更新する
終了

FIG. 35

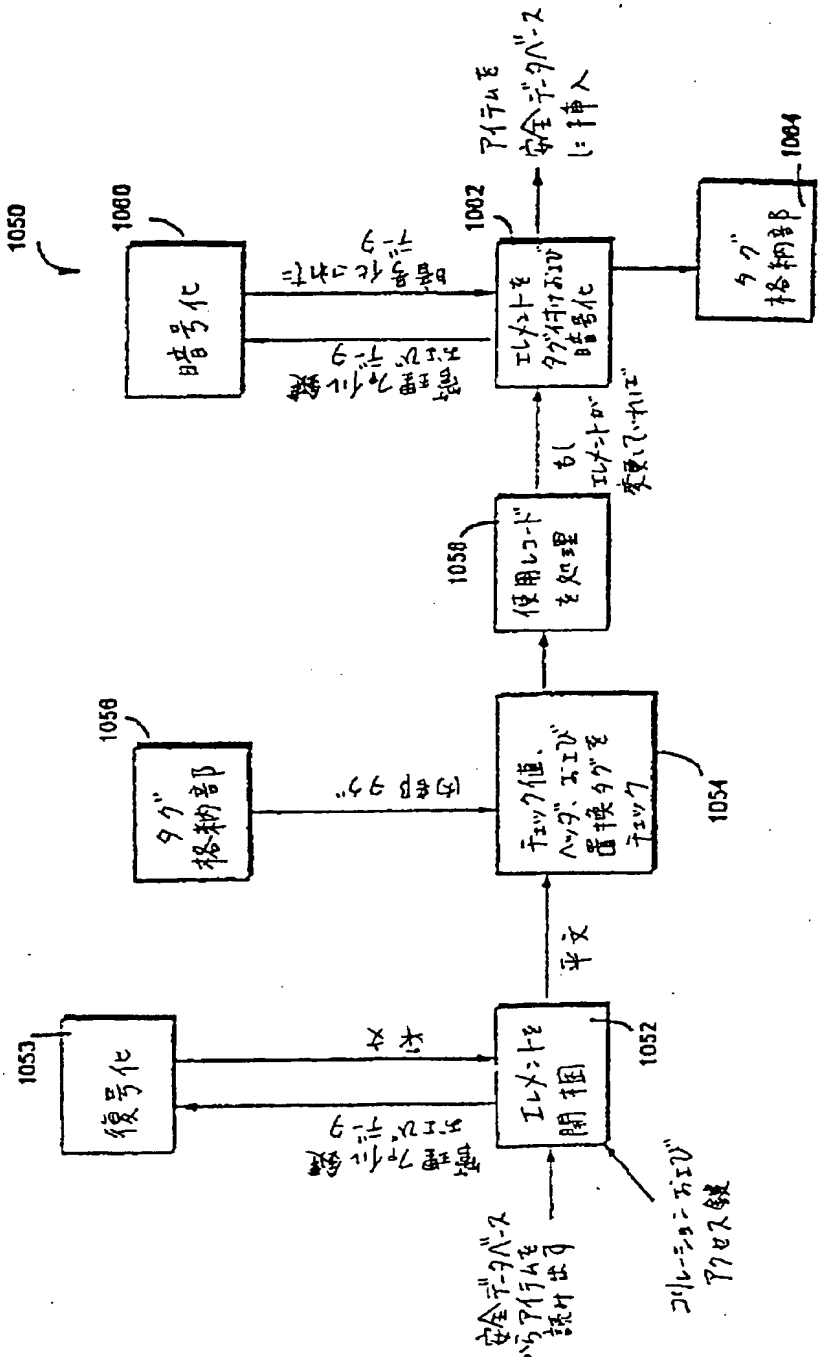
【図３６】

FIG. 36


1080
暗号化
暗号化されたデータ
暗号化されたデータ
1082
アイテムを安全データベースに挿入
1084
タグ格納部
平文
チェック済み
1078
復号化
平文
復号されたデータ
チェック値およびデジタル署名テストにより、エレメントの完全性をチェック
1078
ユーザが認められる
1070
1074
承認サービス
許可
承認されたユーザ
アイテムをデータベースに挿入するためのユーザ承認をチェック
1072
安全データベースに挿入されるアイテムを供給

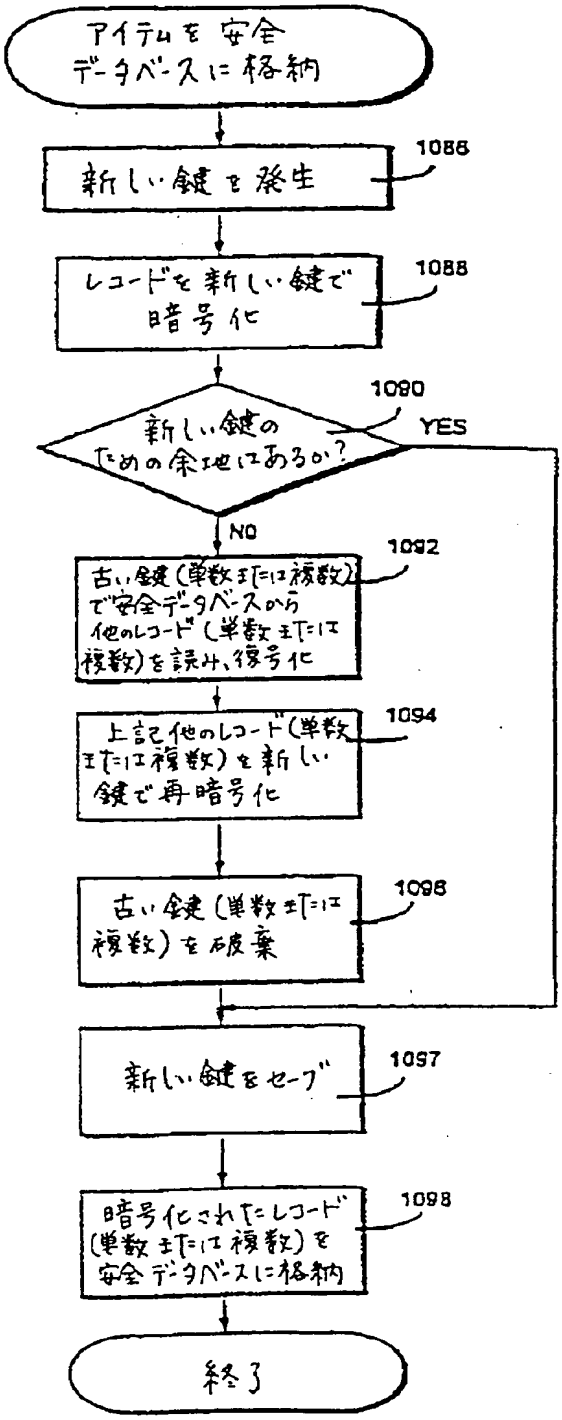
【図３７】

FIG. 37


1050
1060
暗号化
暗号化されたデータ
処理されたデータ
1002
エレメントを
タグ付けされた
暗号化
アイテムを
安全データベース
に挿入
1004
タグ
格納部
もし
エレメントが
変更されていれば
1058
使用レコード
を処理
1058
タグ
格納部
古いタグ
チェック値、
ヘッダ、エレメント
置換タグを
チェック
1054
平文
1053
復号化
平文
処理されたデータ
1052
エレメントを
開梱
安全データベース
からアイテムを
読み出す
コレクション・エレメント
アクセス鍵

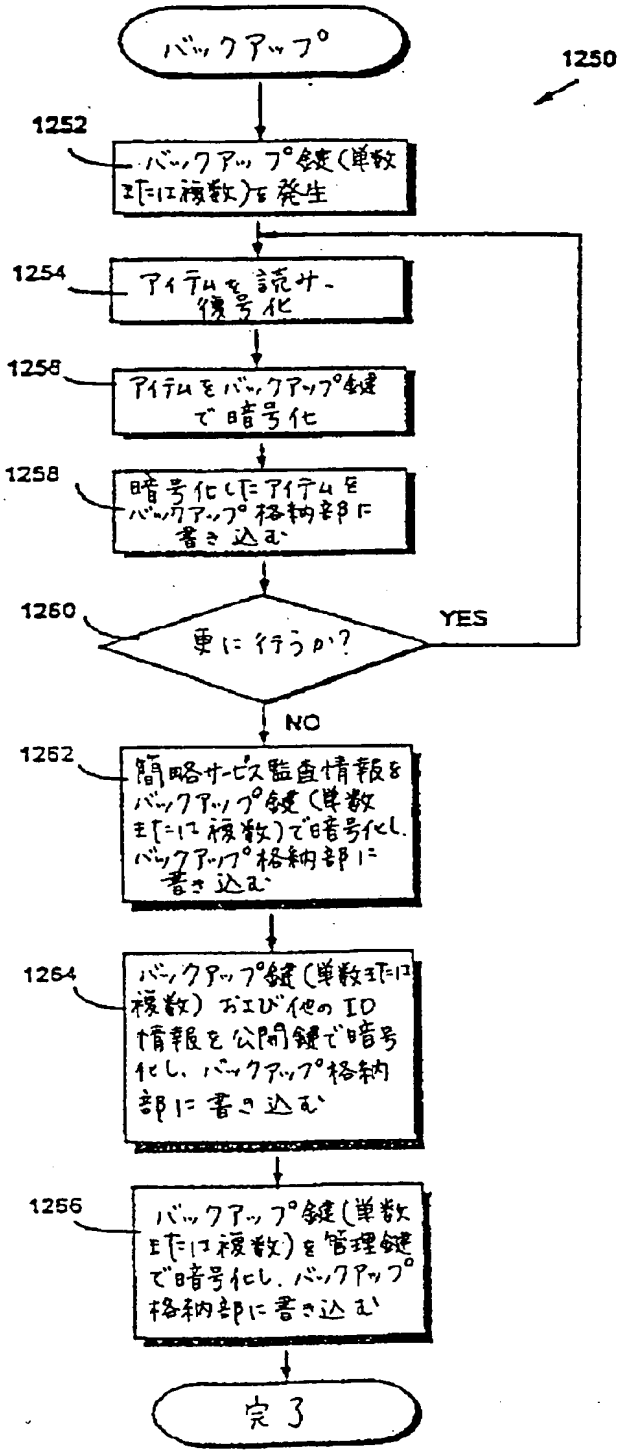
【図３８】

FIG. 38


アイテムを安全データベースに格納
1086
新しい鍵を発生
1088
レコードを新しい鍵で暗号化
1090
新しい鍵のための余地はあるか?
YES
NO
1092
古い鍵(単数または複数)で安全データベースから他のレコード(単数または複数)を読み、復号化
1094
上記他のレコード(単数または複数)を新しい鍵で再暗号化
1096
古い鍵(単数または複数)を破棄
1097
新しい鍵をセーブ
1098
暗号化されたレコード(単数または複数)を安全データベースに格納
終了

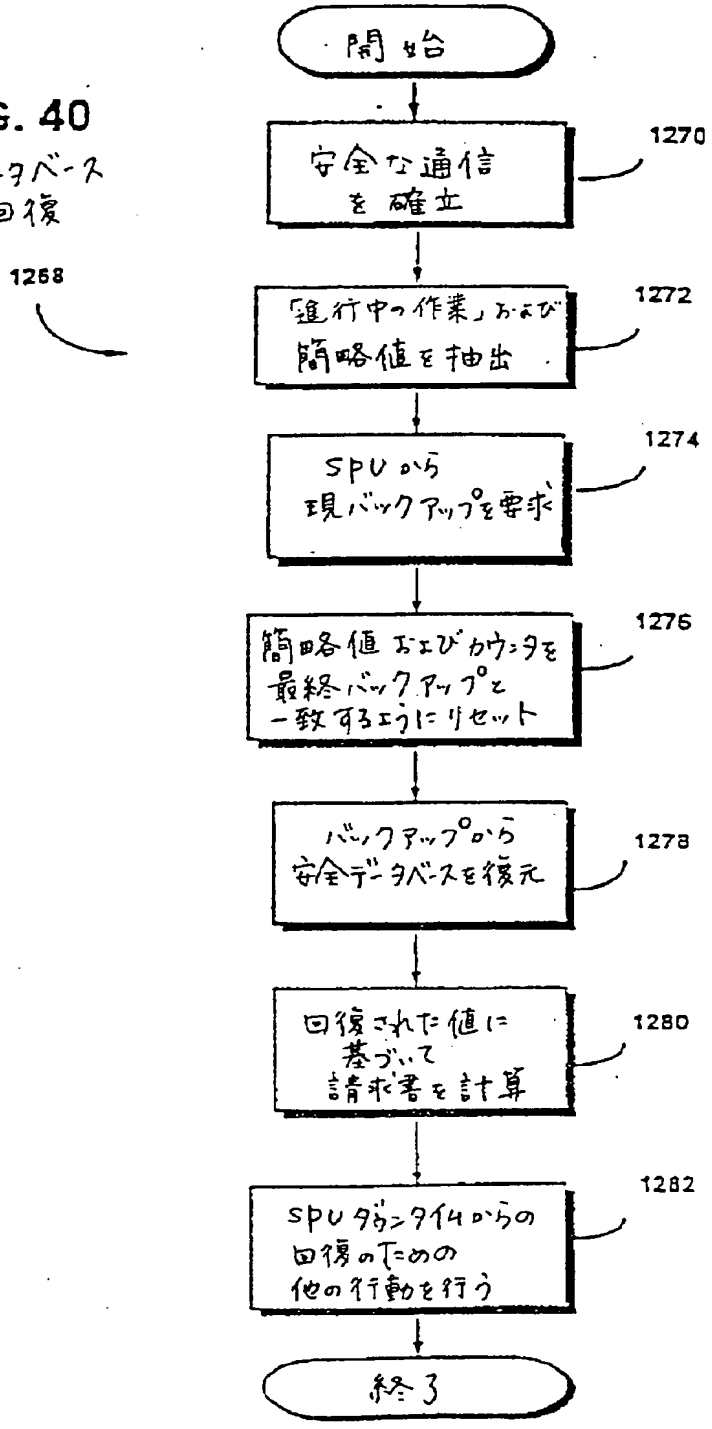
【図３９】

FIG. 39
バックアップ



【図４０】

FIG. 40
安全データベースの回復



【図４１】

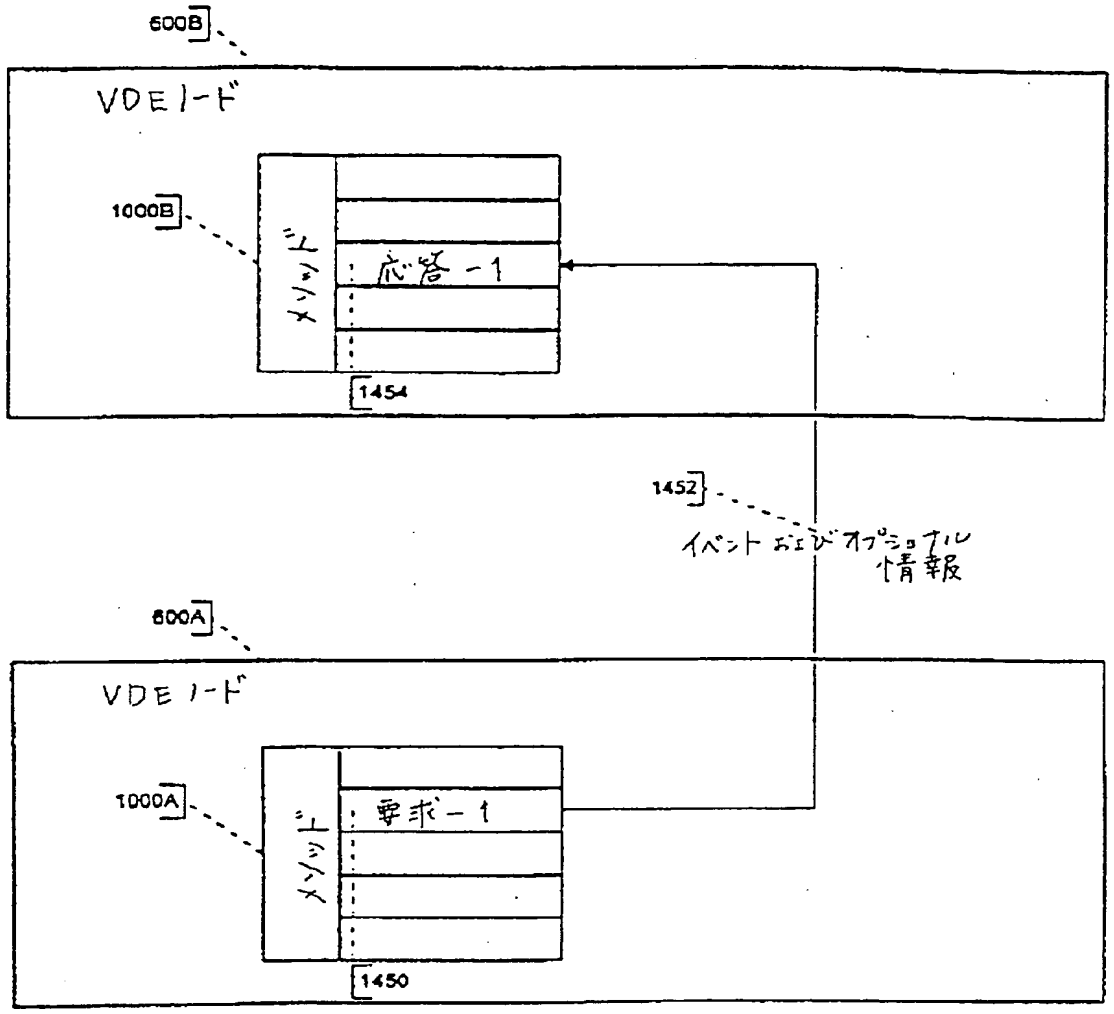


Figure 41a

【図４１】

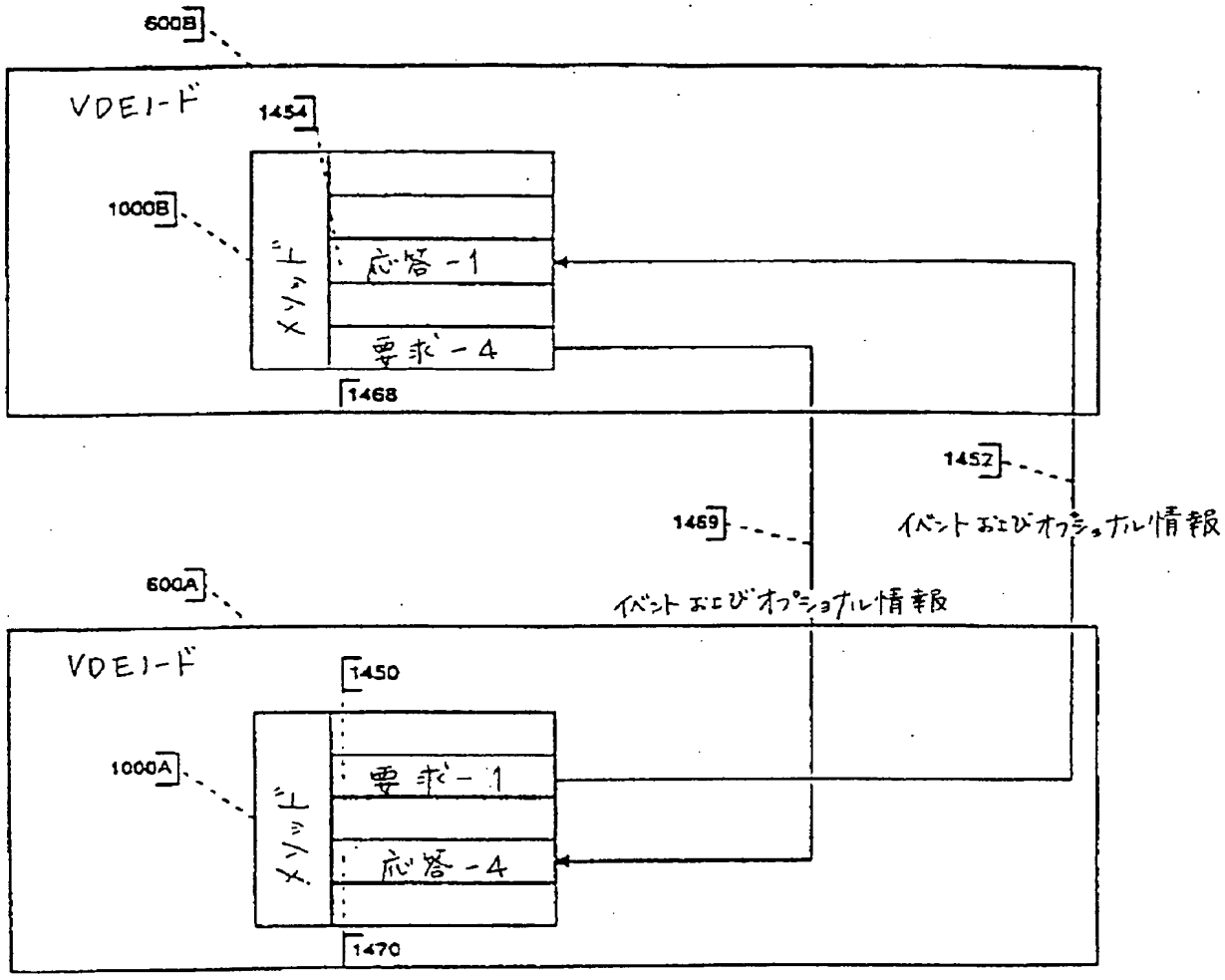


Figure 41b

【図４１】

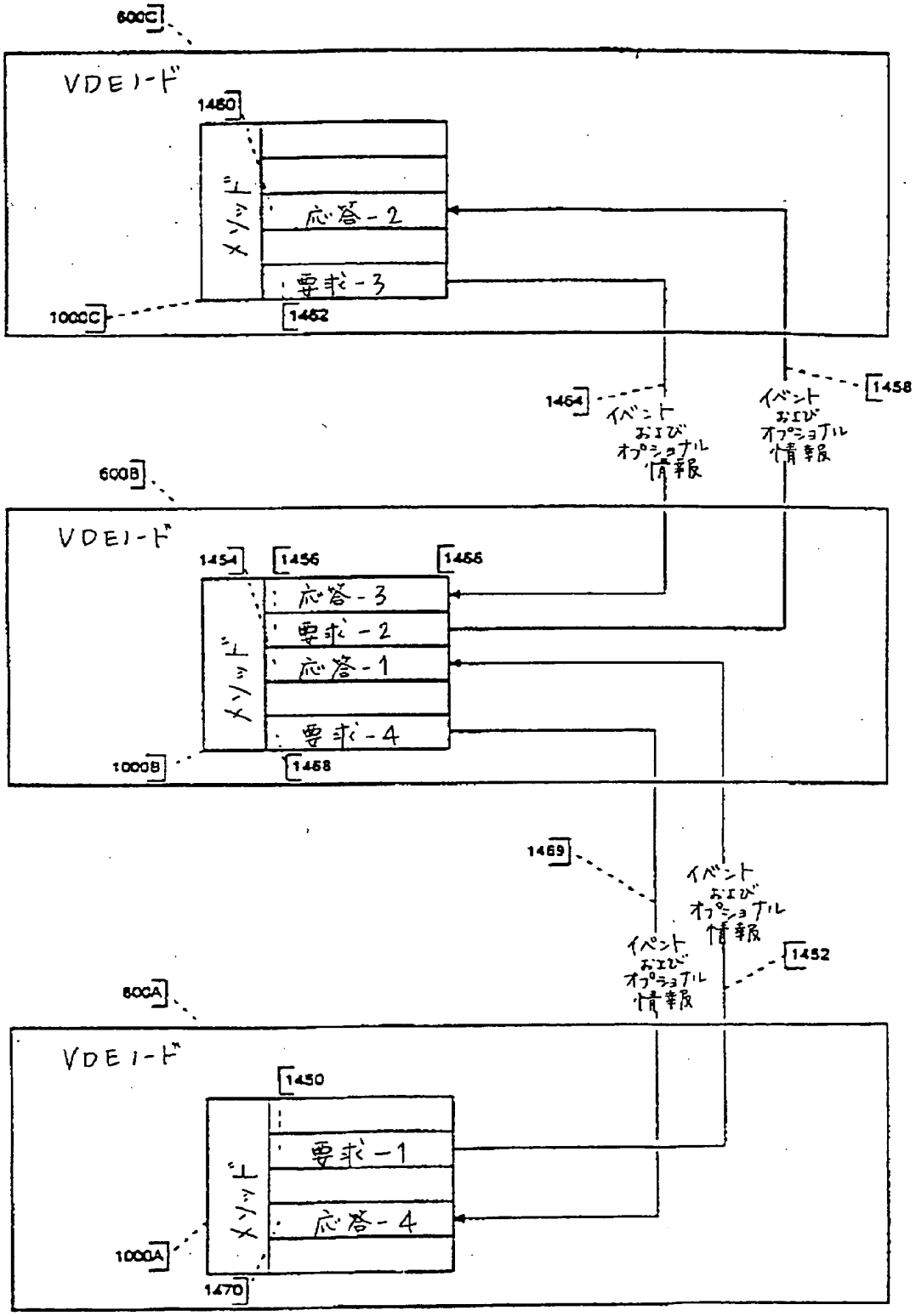


Figure 41c

【図４１】

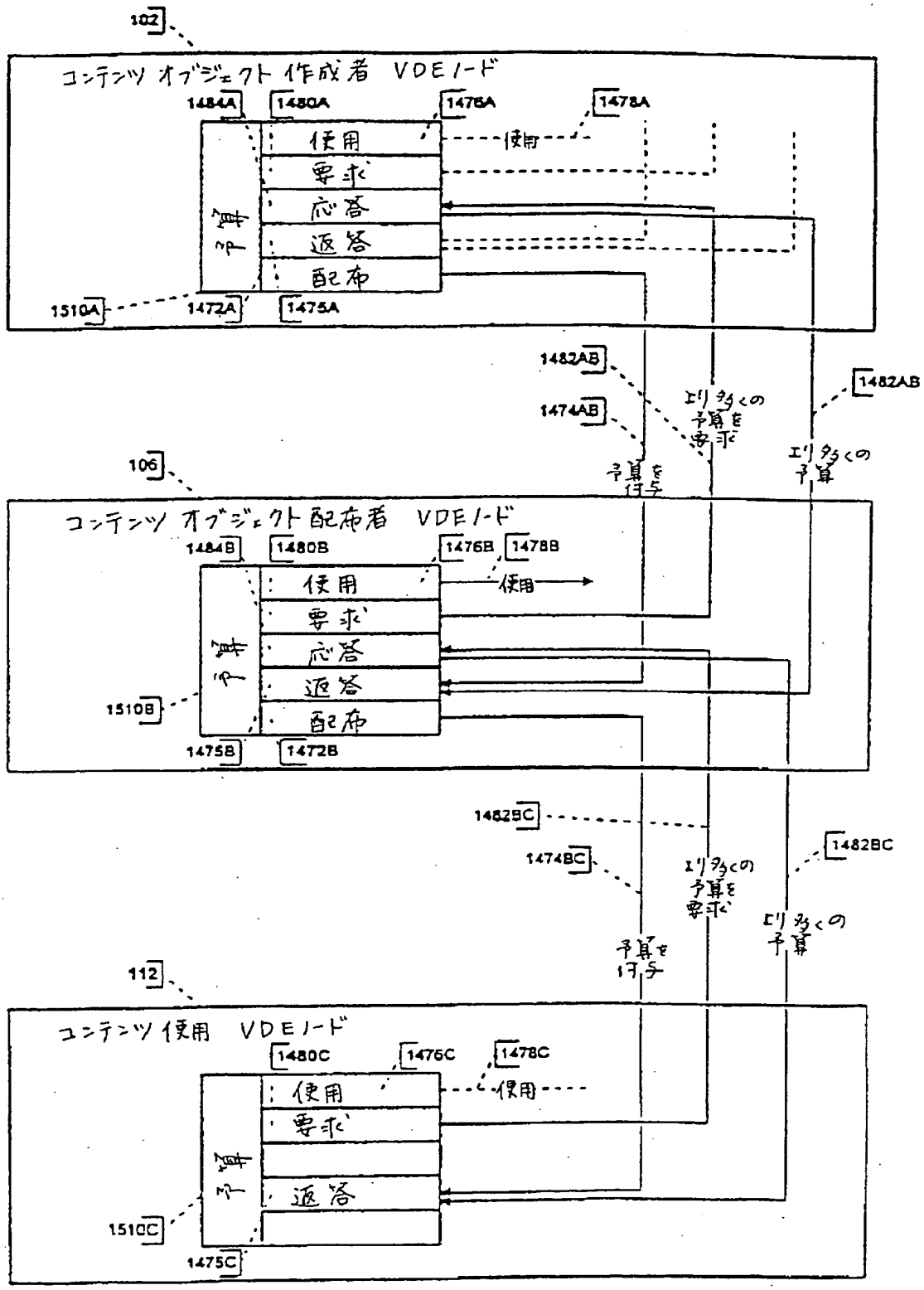
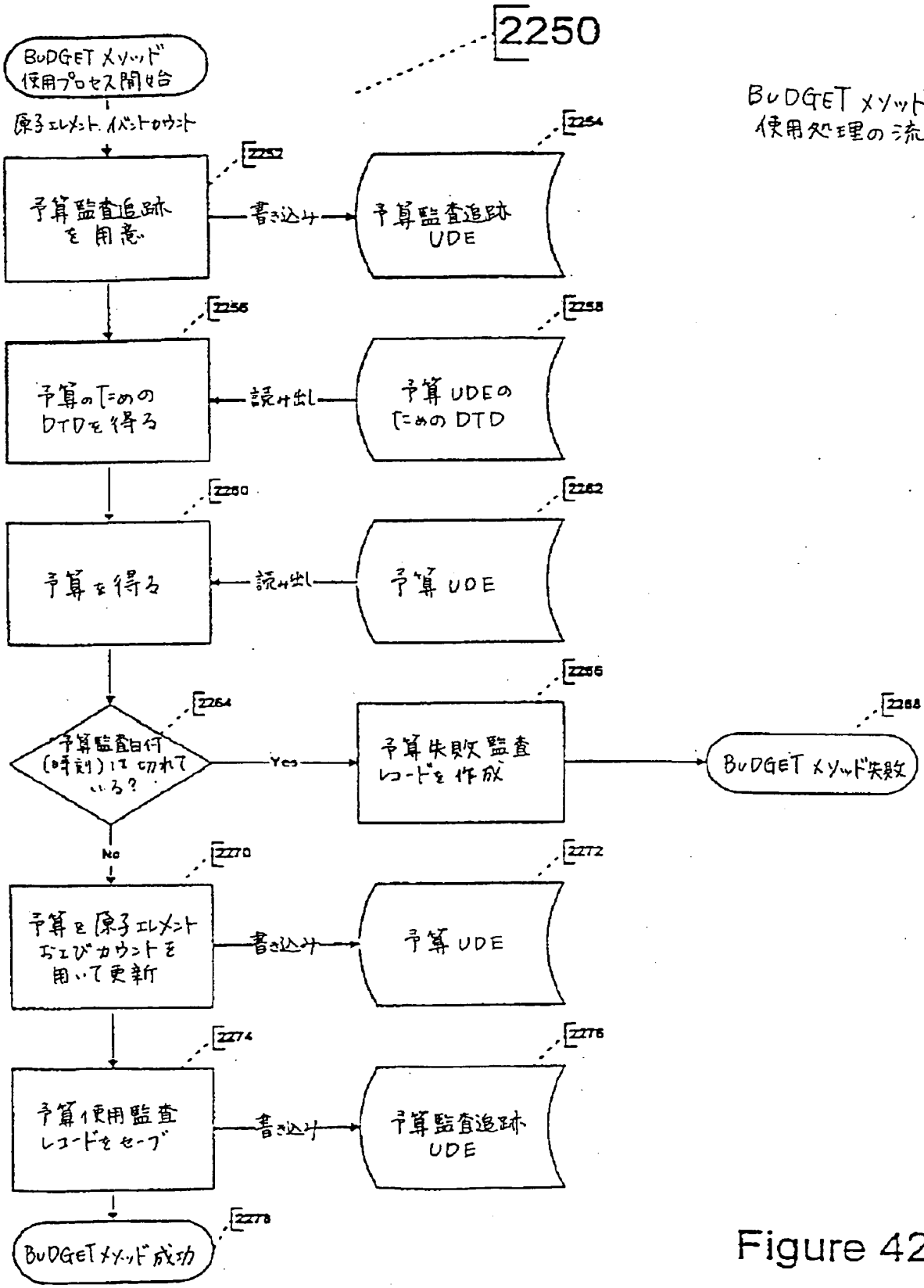


Figure 41d

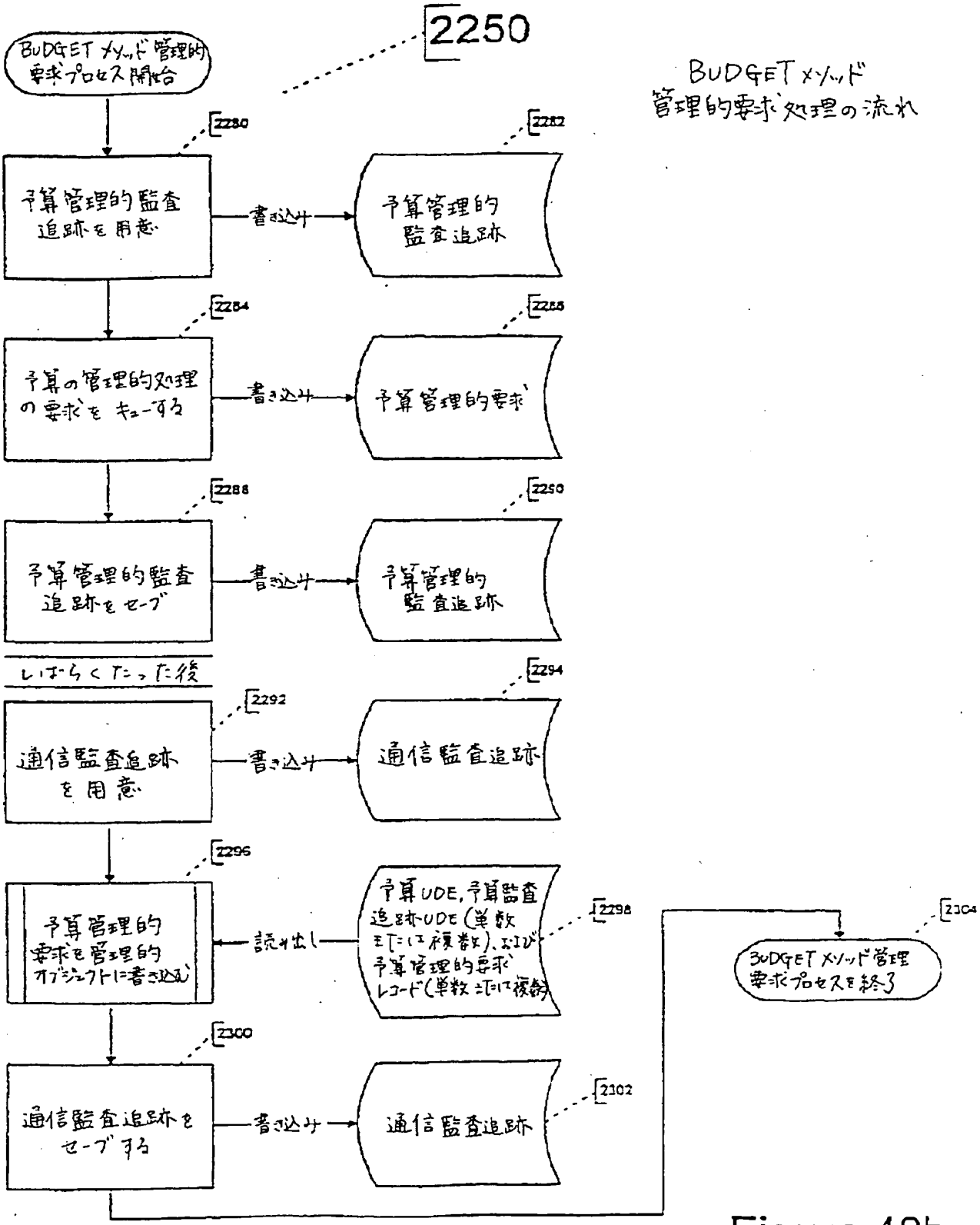
【図42】



BUDGETメソッド使用処理の流れ

Figure 42a

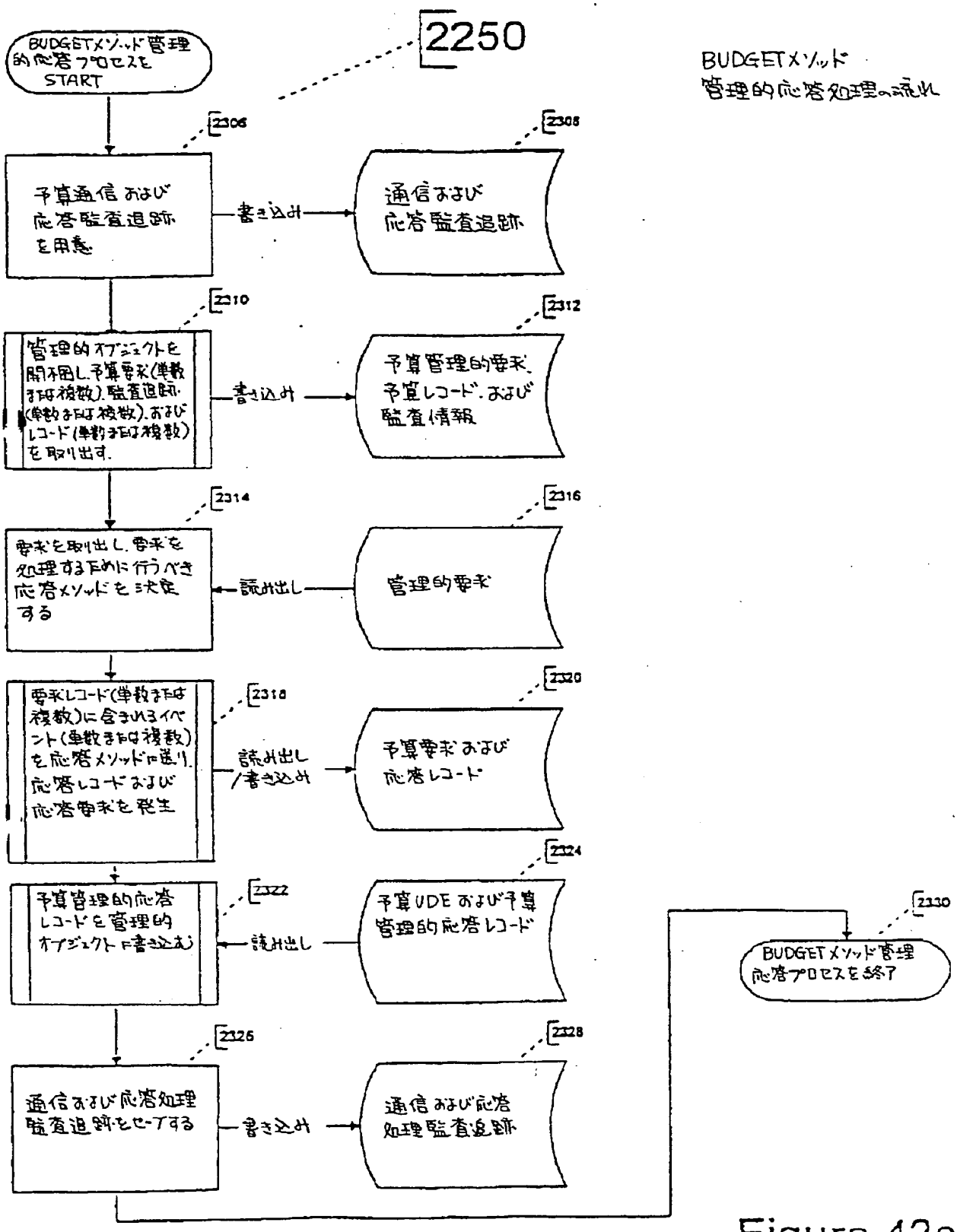
【図42】



BUDGETメソッド管理的要求処理の流れ

Figure 42b

【図４２】



BUDGETメソッド管理的応答処理の流れ

Figure 42c

【図４２】

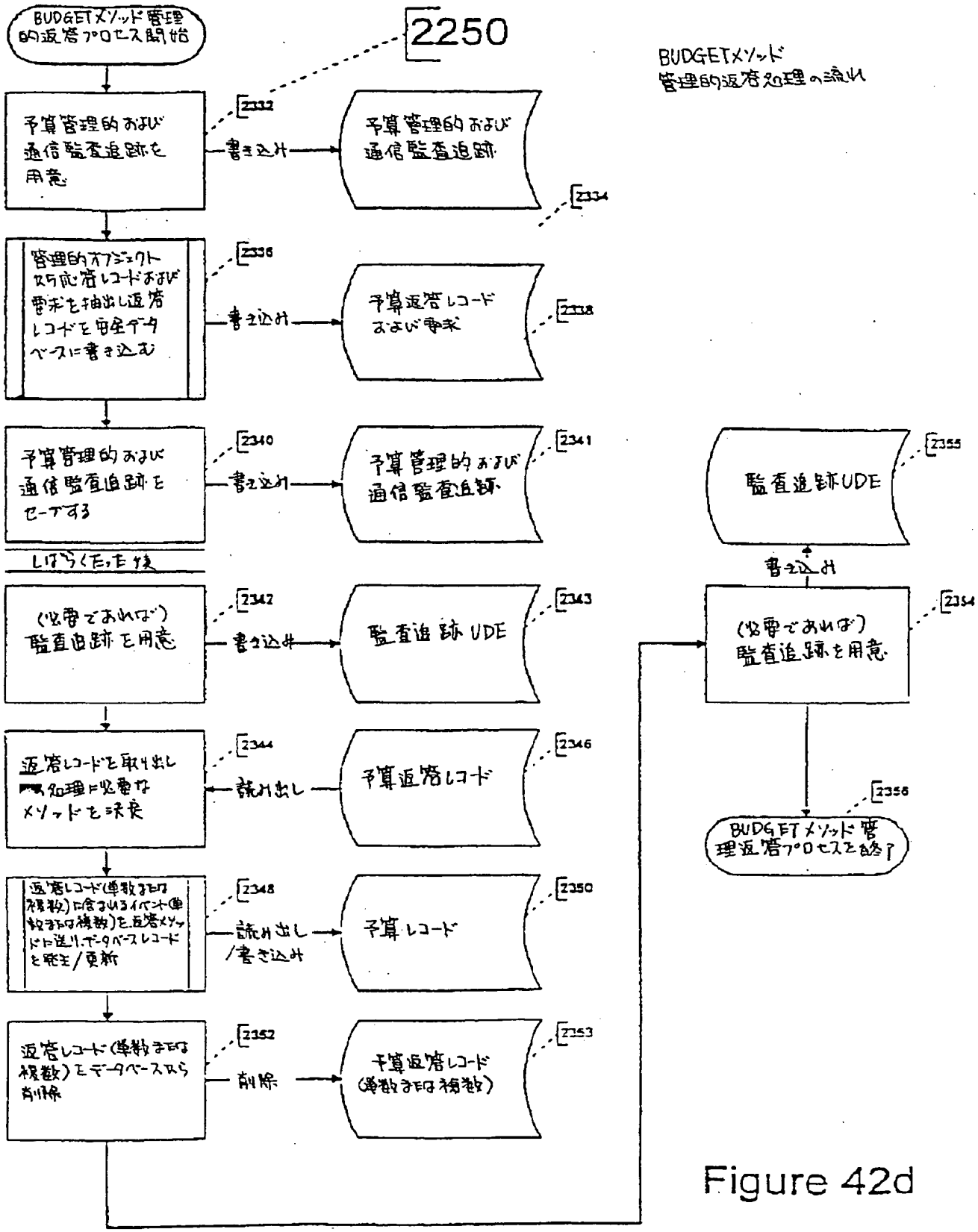


Figure 42d

【図４３】

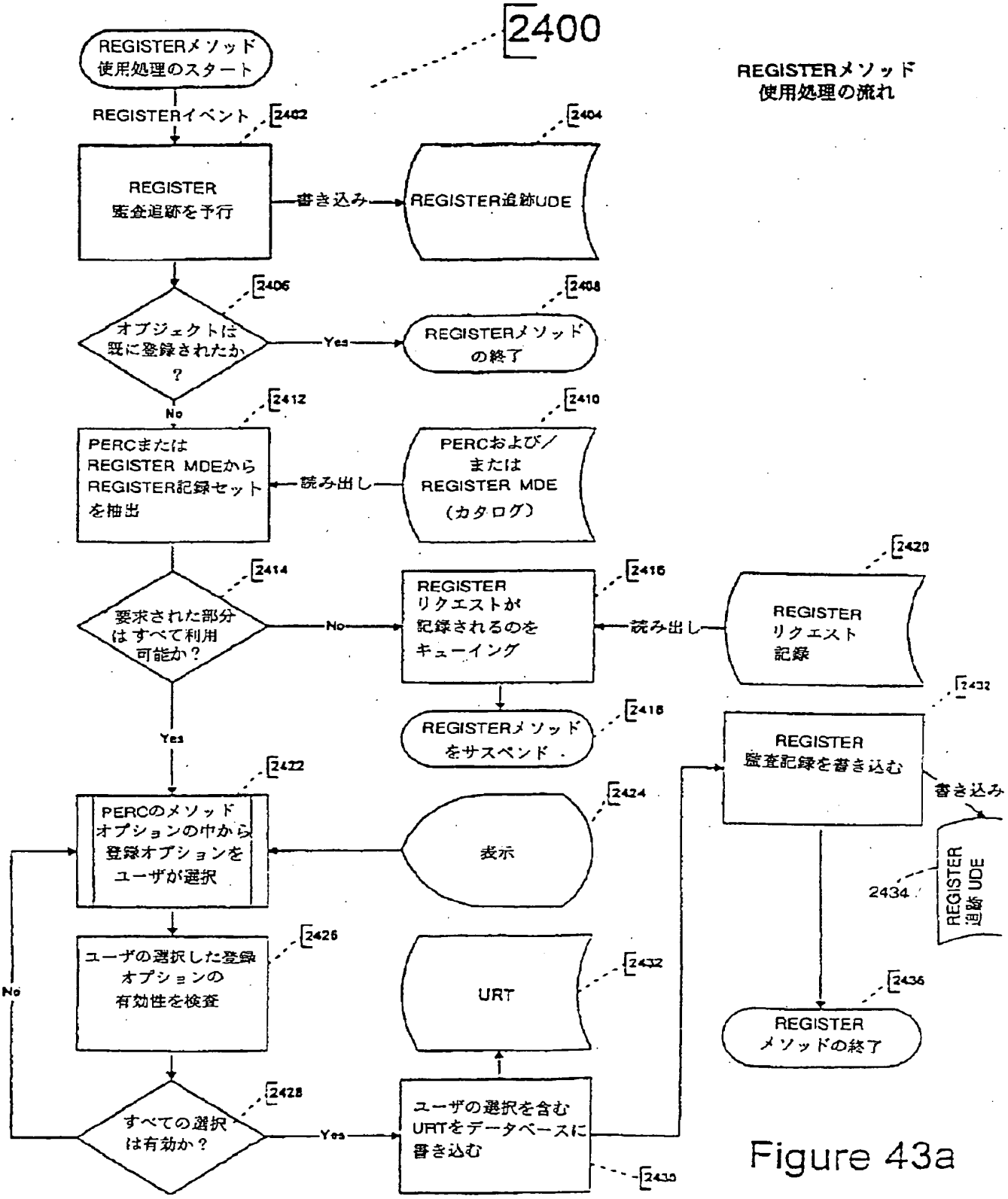
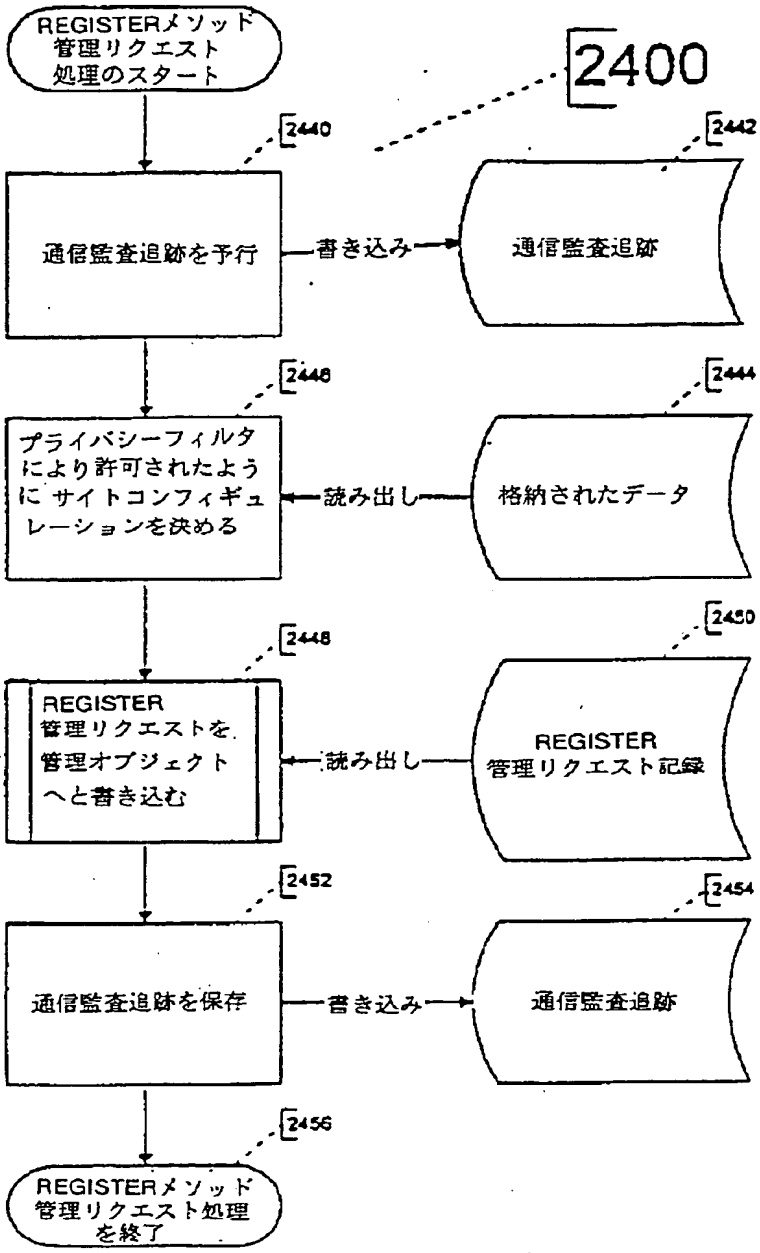


Figure 43a

【図４３】



REGISTERメソッド
管理リクエスト処理の流れ

Figure 43b

【図４３】

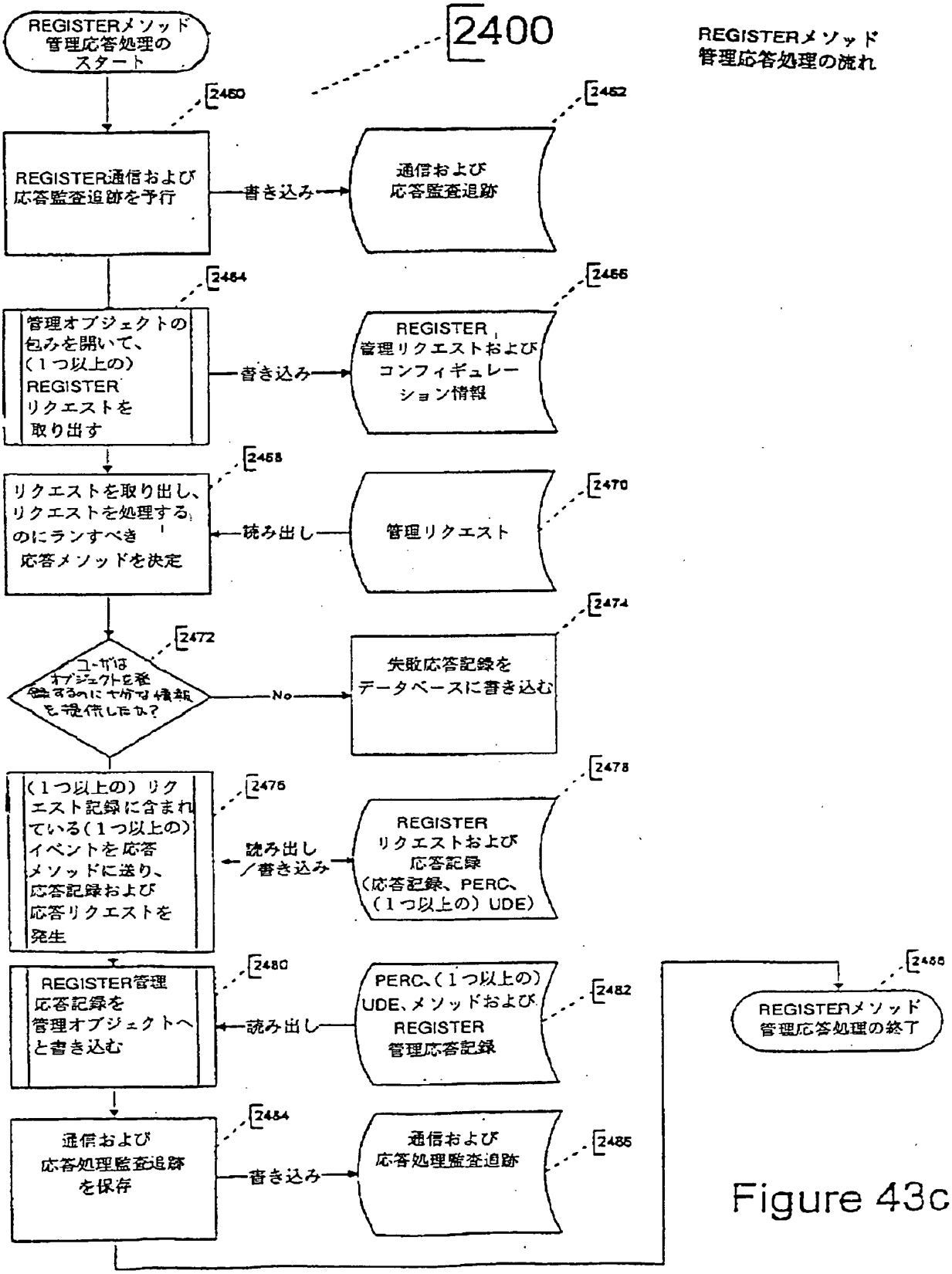


Figure 43c

【図４３】

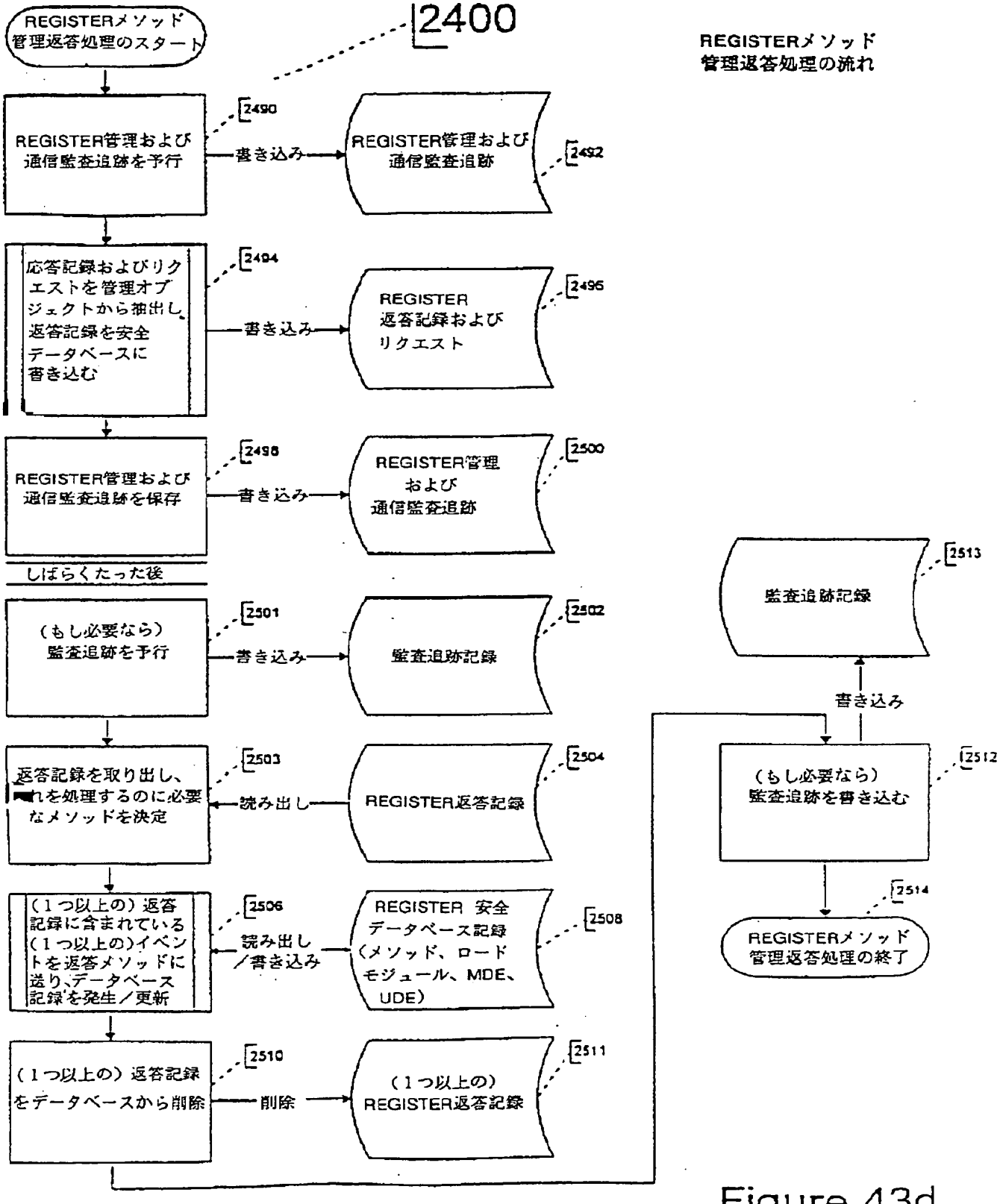


Figure 43d

【図４４】

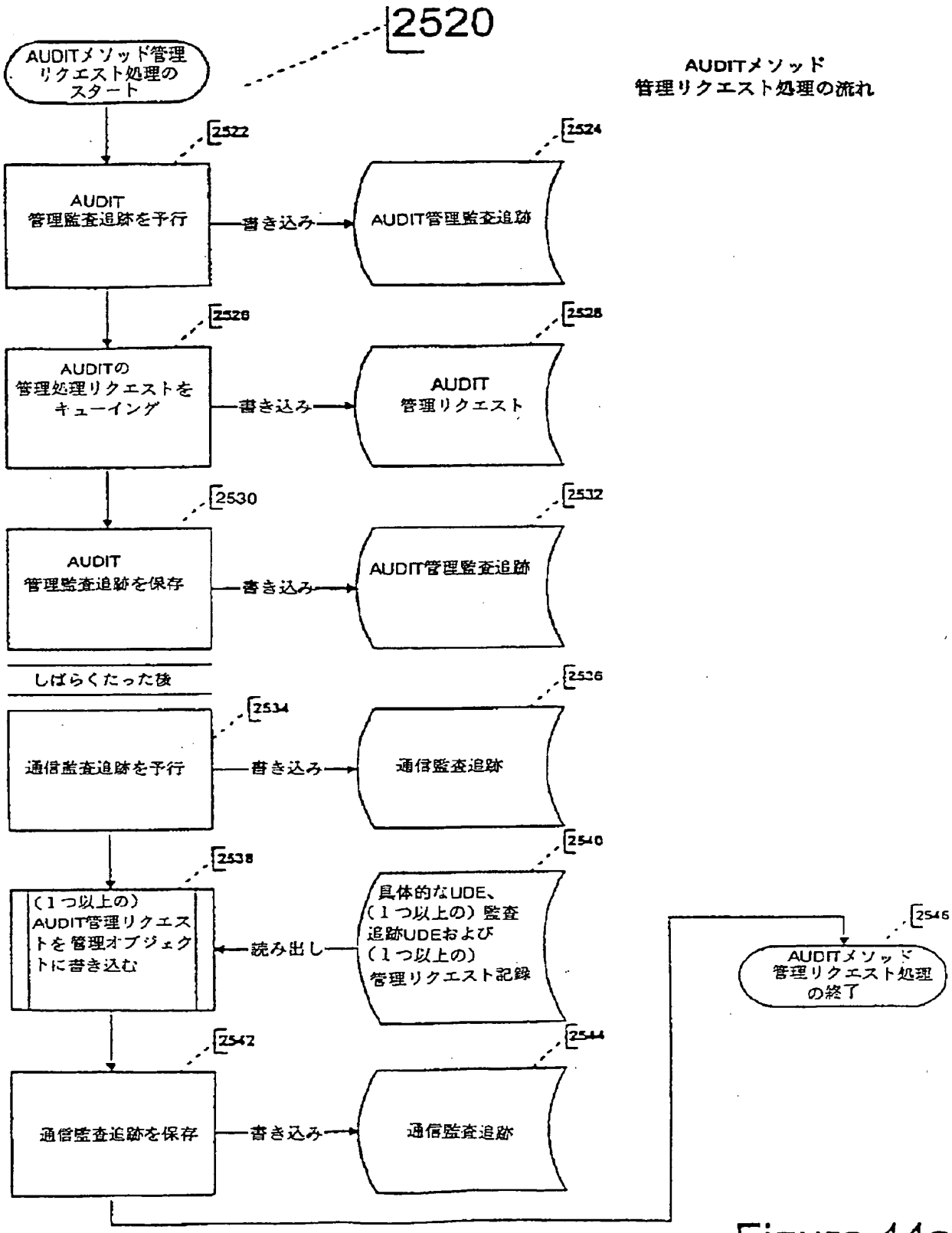


Figure 44a

【図４４】

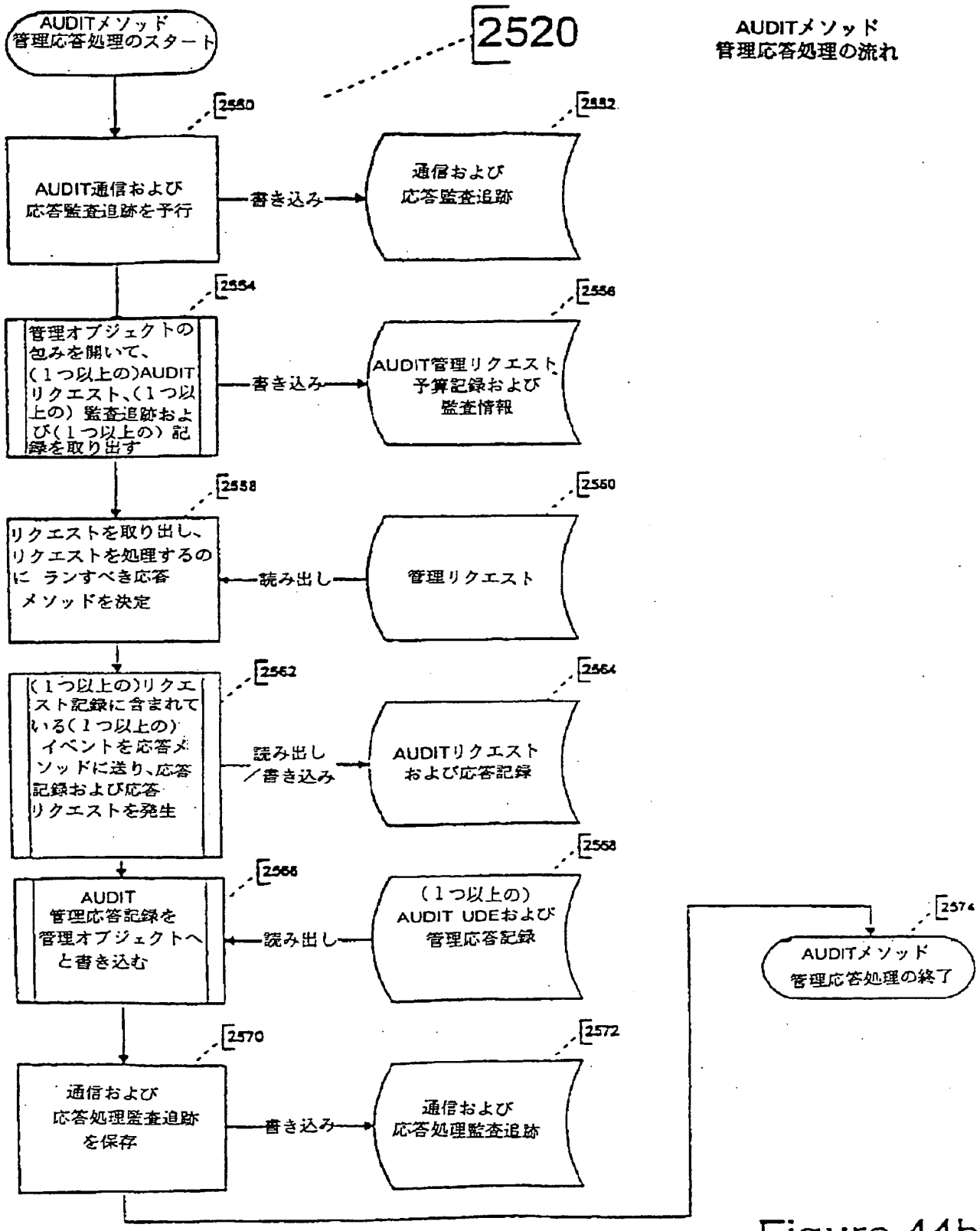


Figure 44b

【図４４】

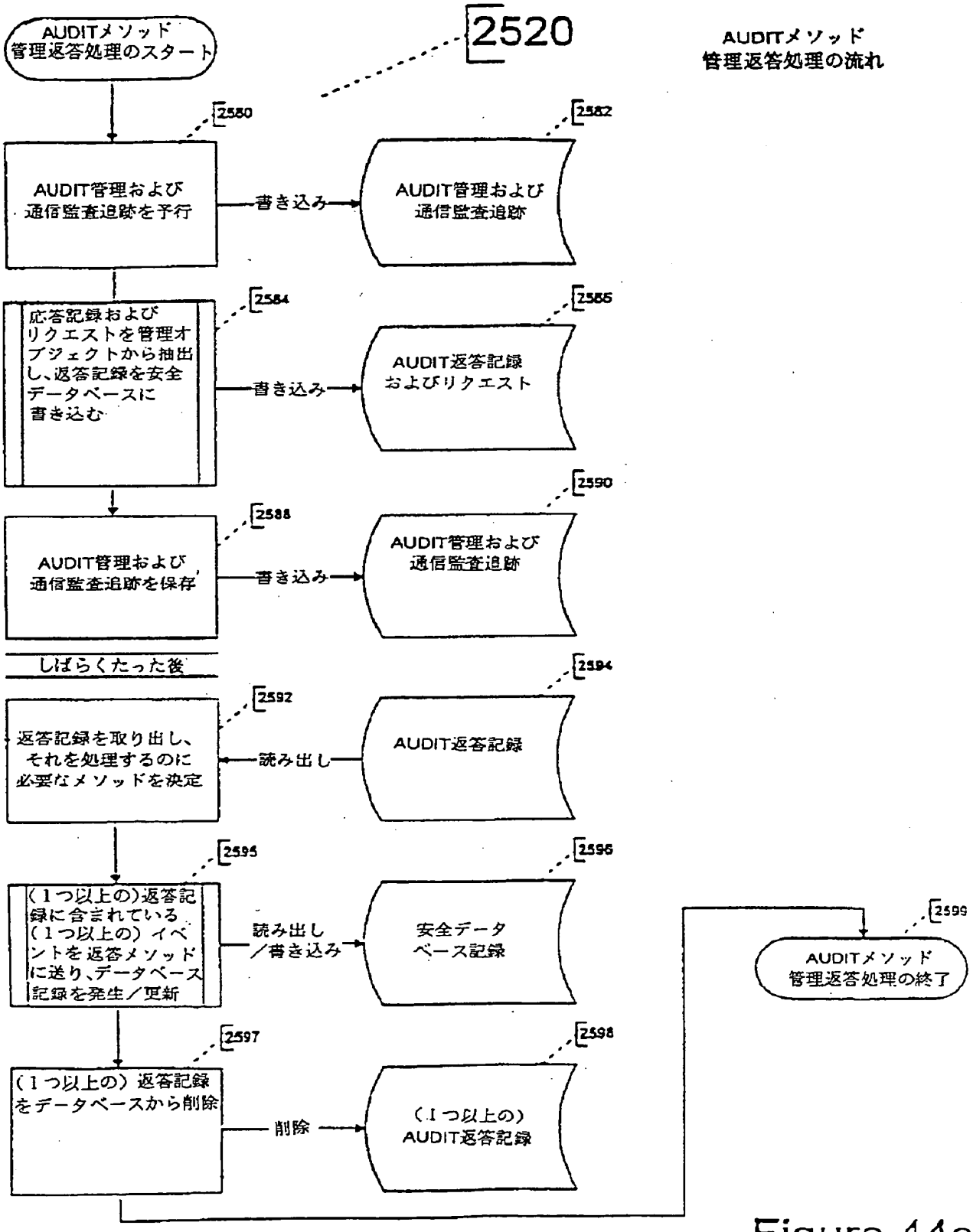
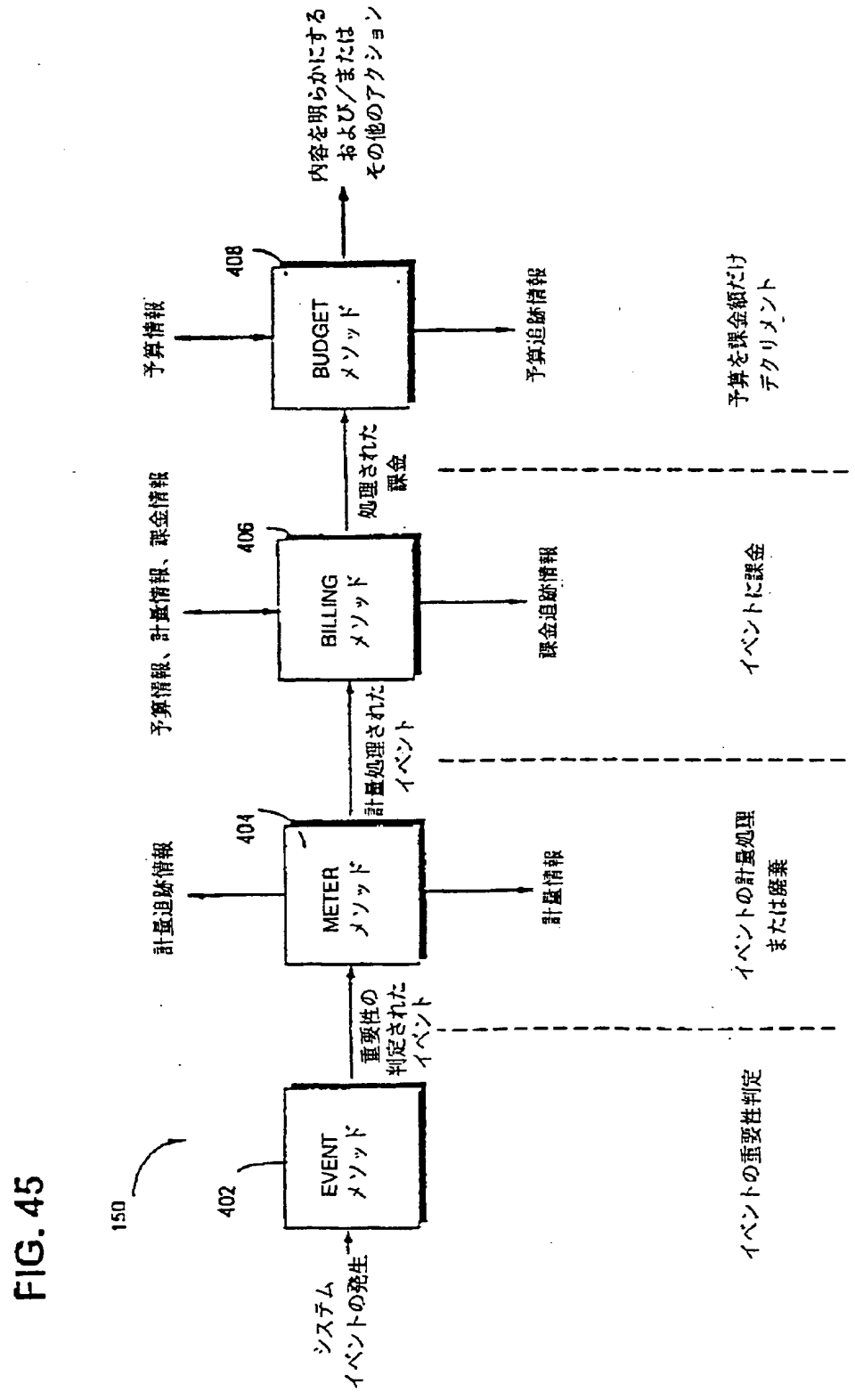


Figure 44c

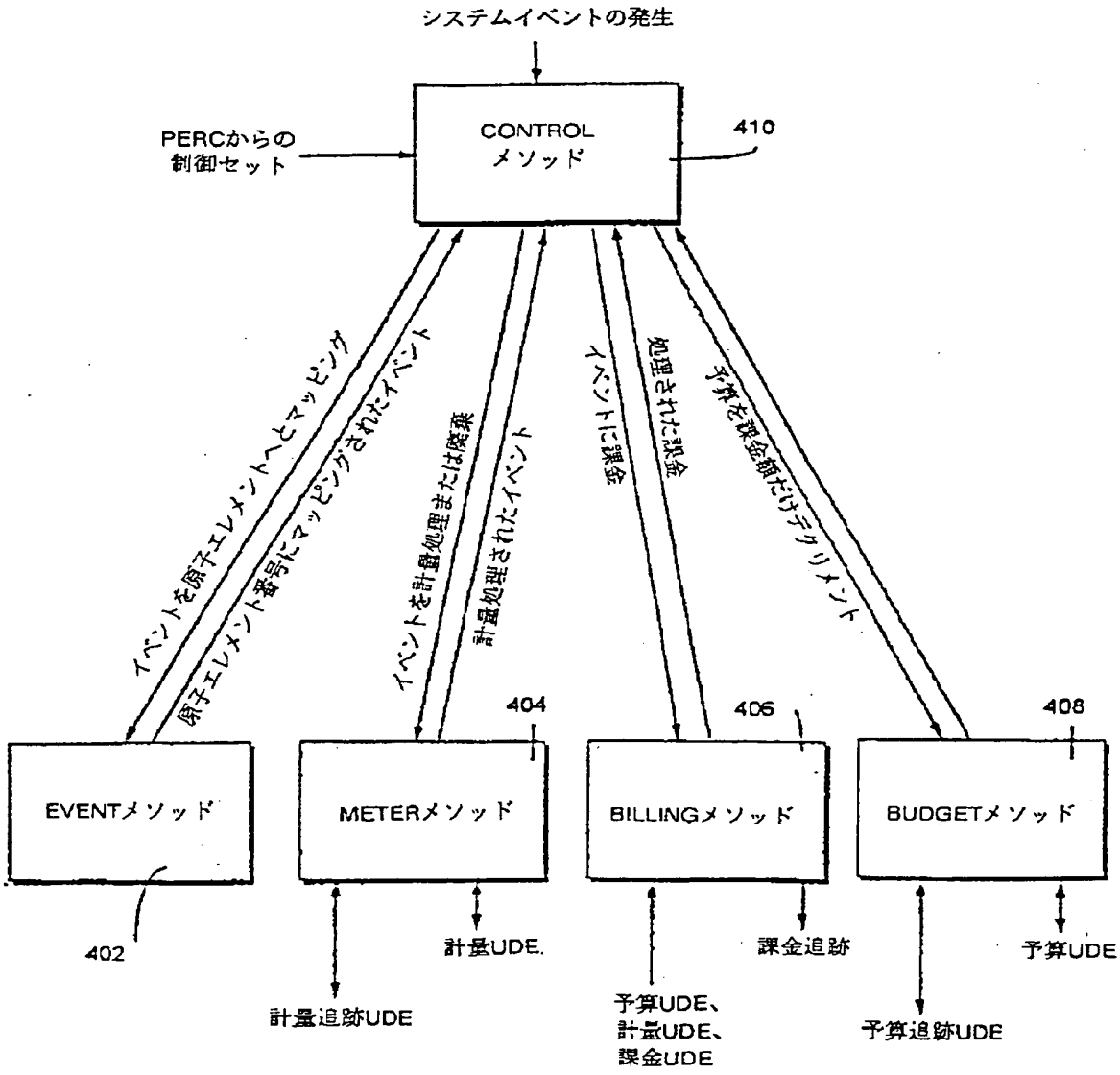
【図45】

FIG. 45


150
402
EVENT
メソッド
404
METER
メソッド
406
BILLING
メソッド
408
BUDGET
メソッド
システム
イベントの発生
重要性の
判定された
イベント
計量処理された
イベント
処理された
課金
内容を明らかにする
および/または
その他のアクション
計量追跡情報
予算情報
予算情報、計量情報、課金情報
計量情報
課金追跡情報
予算追跡情報
イベントの重要性判定
イベントの計量処理
または廃棄
イベントに課金
予算を課金額だけ
デクリメント

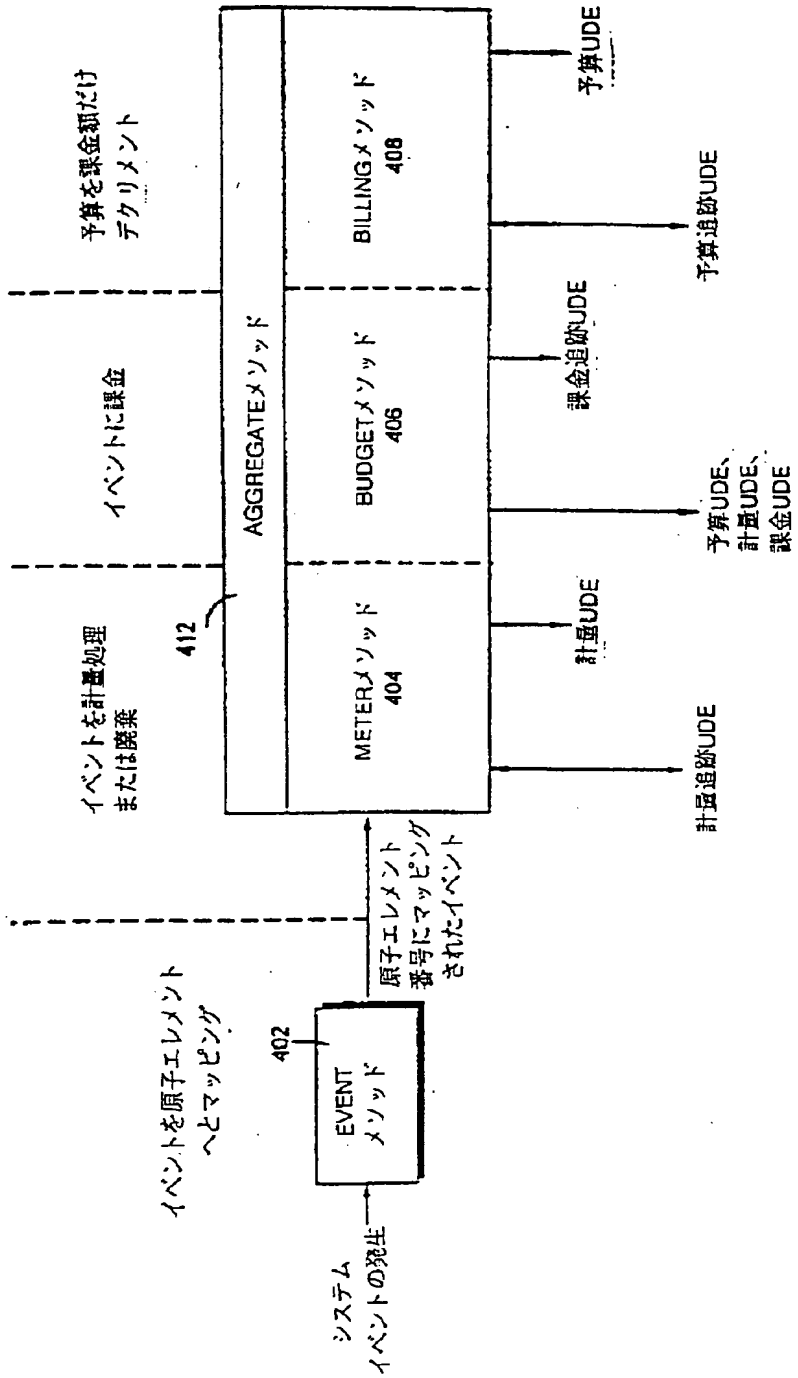
【図４６】

FIG. 46


システムイベントの発生
CONTROL
メソッド
410
PERCからの
制御セット
イベントを原子エレメントへとマッピング
原子エレメント番号にマッピングされたイベント
イベントを計量処理または廃棄
計量処理されたイベント
イベントに課金
処理された課金
予算を課金額だけデクリメント
EVENTメソッド
METERメソッド
BILLINGメソッド
BUDGETメソッド
402
404
406
408
計量追跡UDE
計量UDE
予算UDE、
計量UDE、
課金UDE
課金追跡
予算追跡UDE
予算UDE

【図47】

FIG. 47


システム
イベントの発生
EVENT
メソッド
402
イベントを原子エレメント
へとマッピング
原子エレメント
番号にマッピング
されたイベント
412
イベントを計量処理
または廃棄
イベントに課金
予算を課金額だけ
デクリメント
METERメソッド
404
BUDGETメソッド
406
AGGREGATEメソッド
BILLINGメソッド
408
計量追跡UDE
計量UDE
予算UDE、
計量UDE、
課金UDE
課金追跡UDE
予算追跡UDE
予算UDE

【図48】

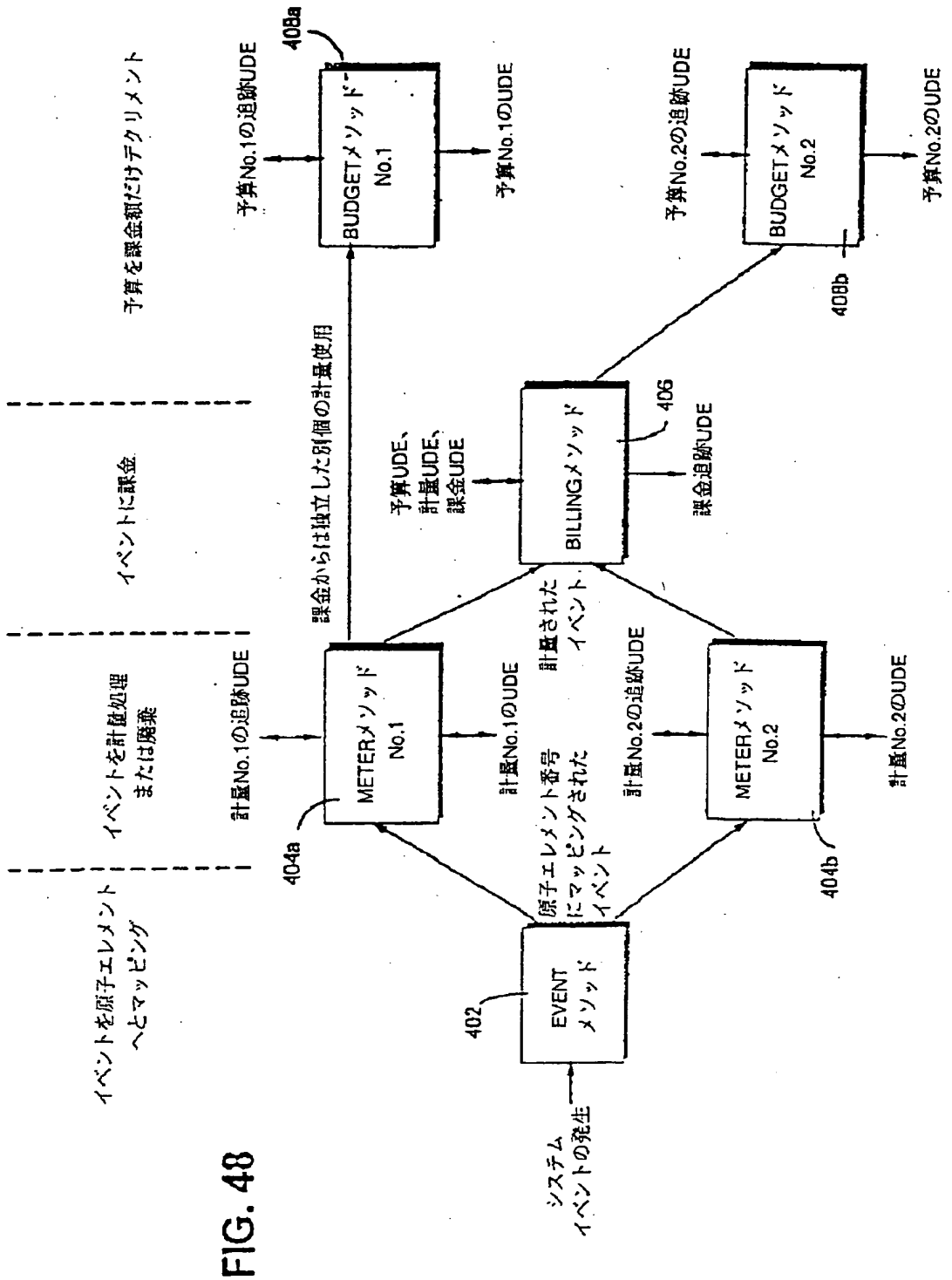

予算を課金額だけデクリメント
イベントに課金
イベントを計量処理または廃棄
イベントを原子エレメントへとマッピング
予算No.1の追跡UDE
BUDGETメソッド No.1
予算No.1のUDE
408a
予算No.2の追跡UDE
BUDGETメソッド No.2
予算No.2のUDE
408b
課金からは独立した別個の計量使用
予算UDE、計量UDE、課金UDE
BILLINGメソッド
406
課金追跡UDE
計量No.1の追跡UDE
METERメソッド No.1
計量No.1のUDE
計量されたイベント
計量No.2の追跡UDE
METERメソッド No.2
計量No.2のUDE
404a
404b
原子エレメント番号にマッピングされたイベント
EVENT メソッド
402
システムイベントの発生

FIG. 48

【図４９】

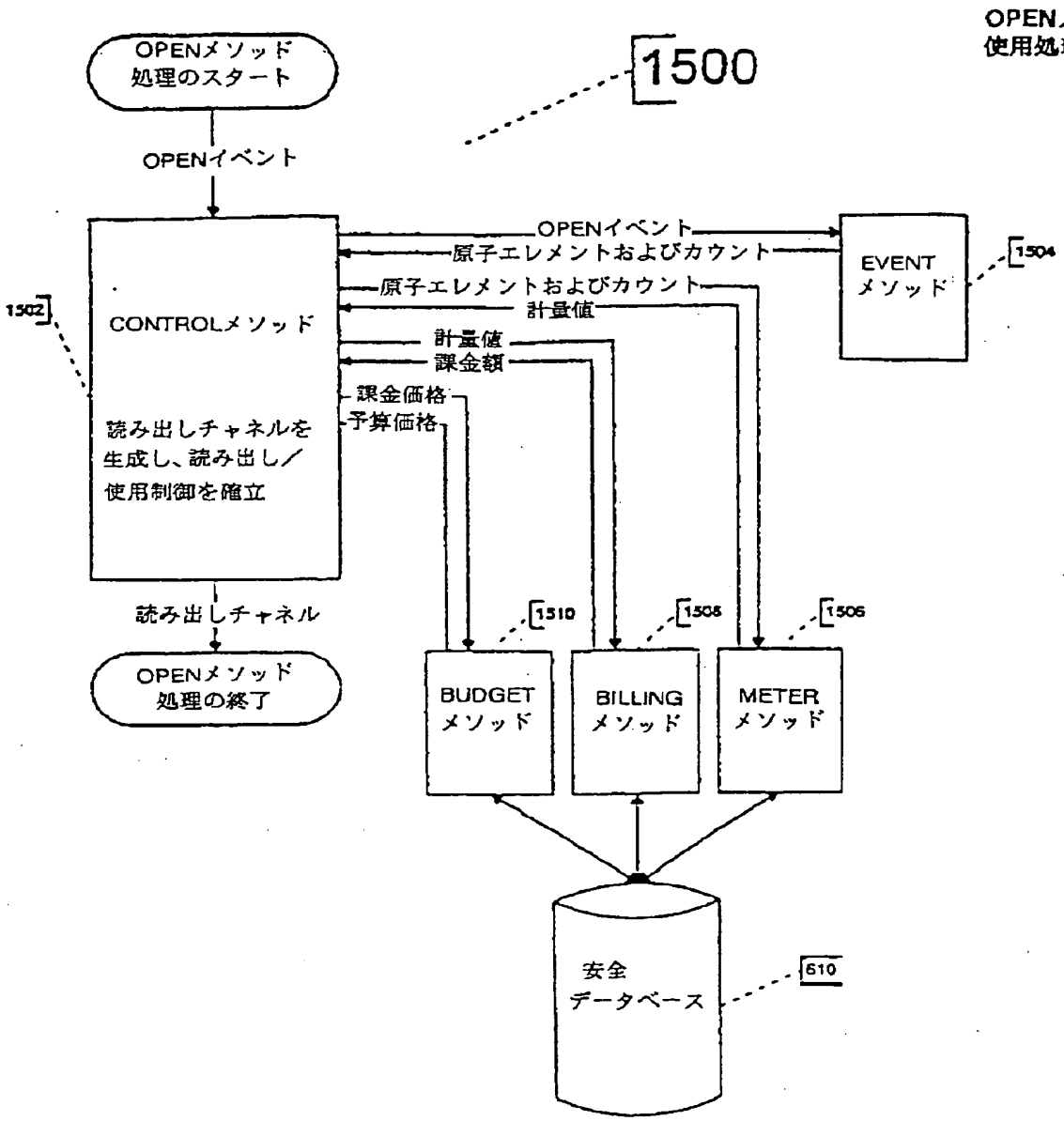


Figure 49

【図４９】

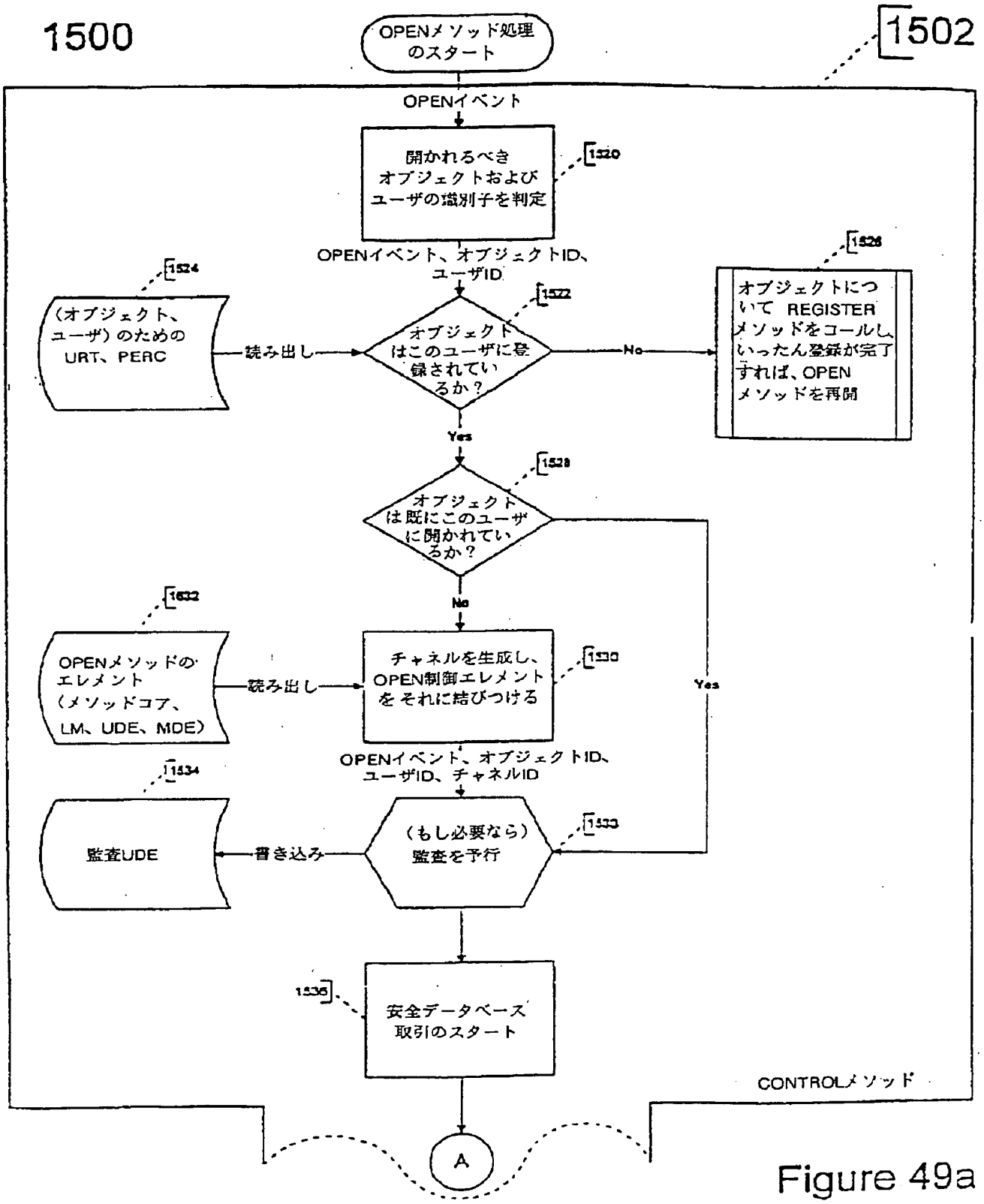


Figure 49a

【図４９】

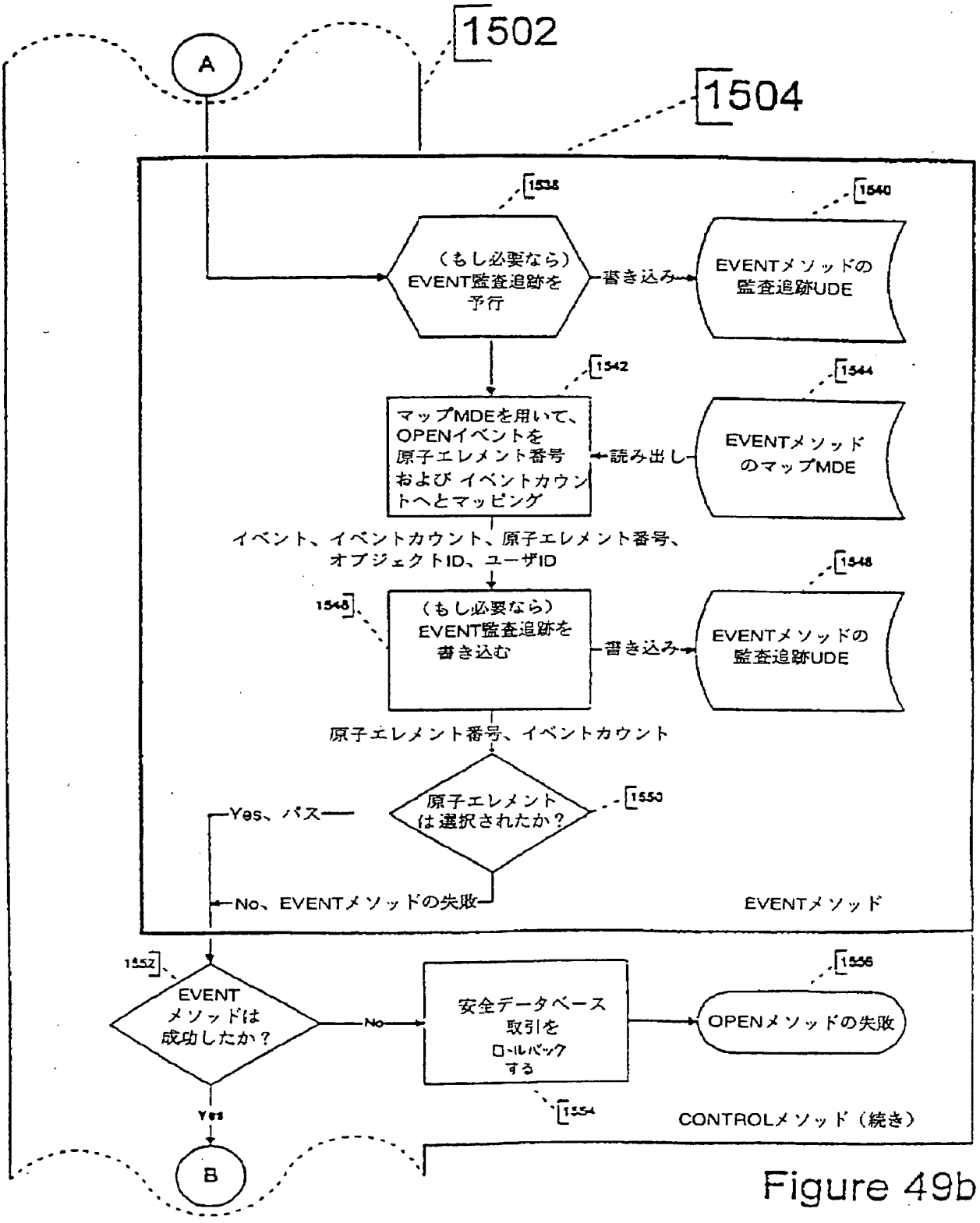


Figure 49b

【図４９】

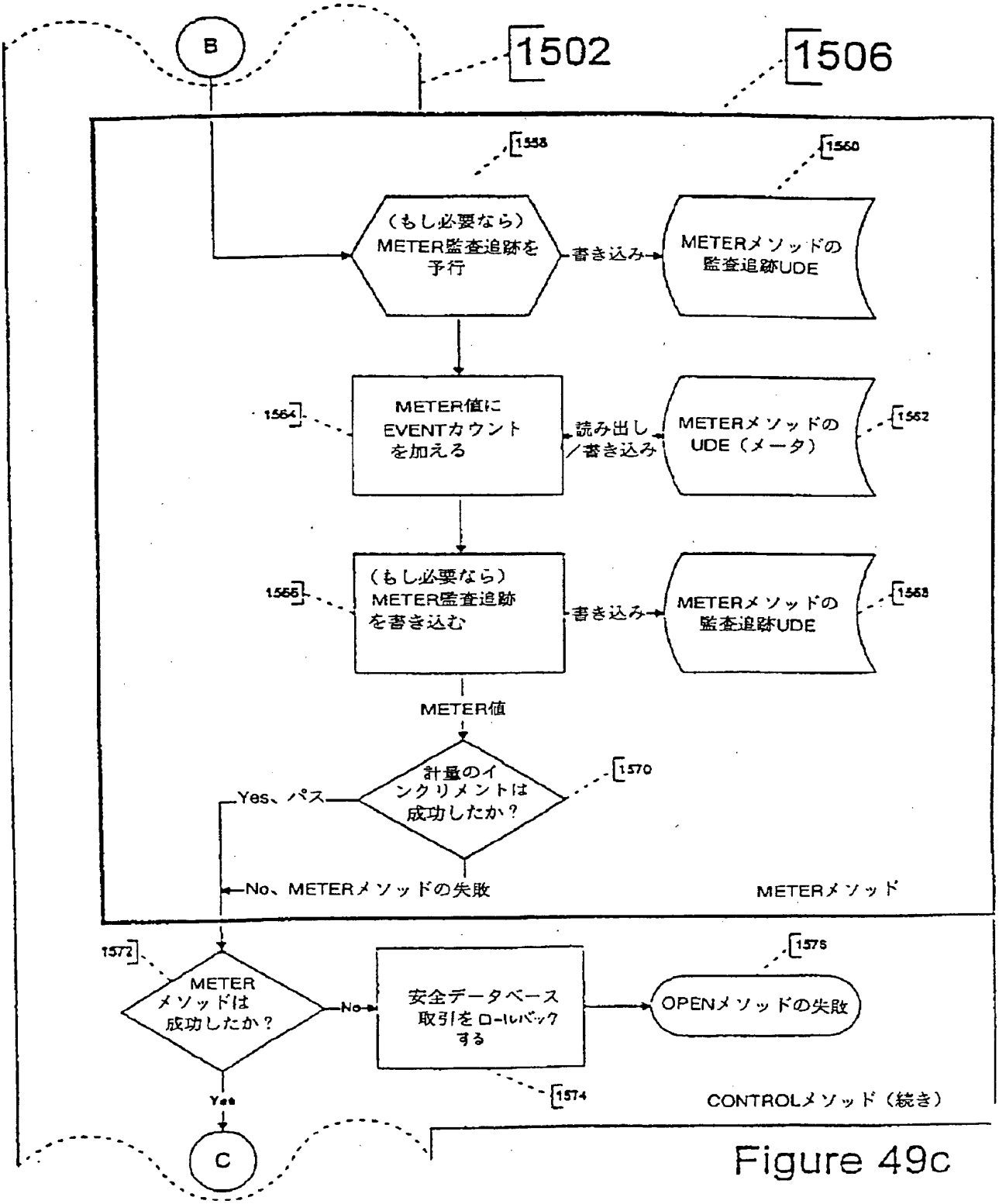


Figure 49c

【図４９】

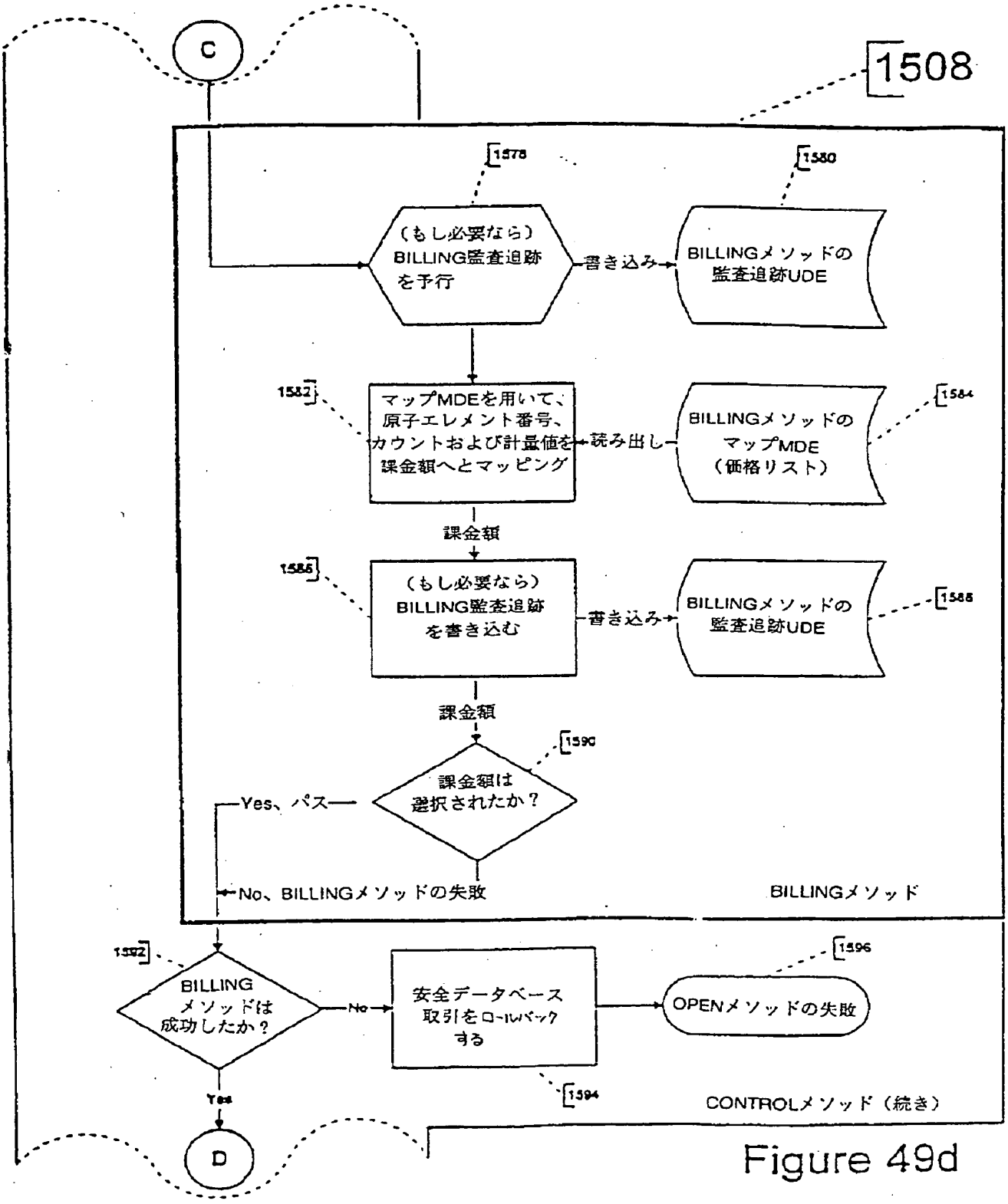


Figure 49d

【図４９】

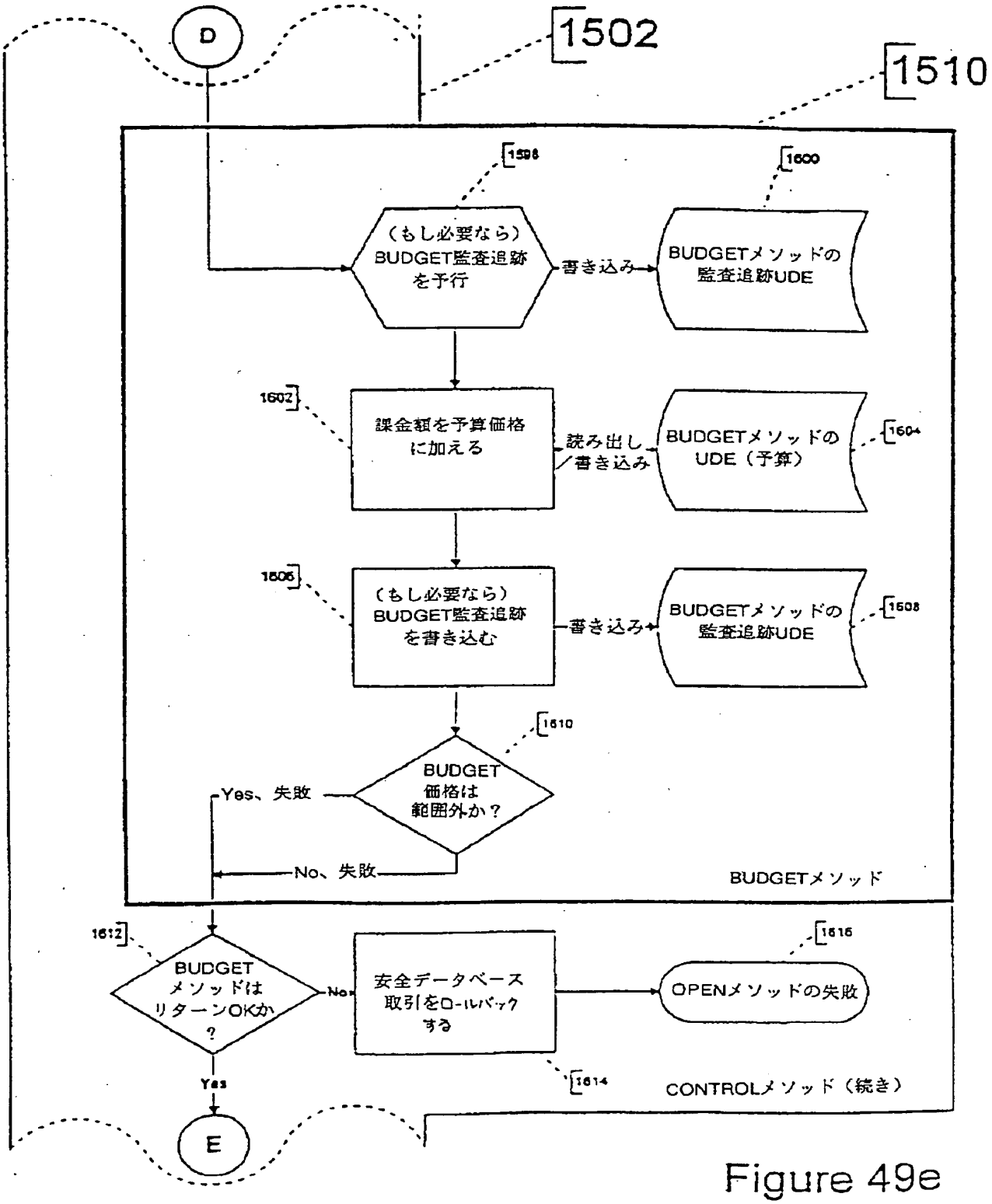


Figure 49e

【図４９】

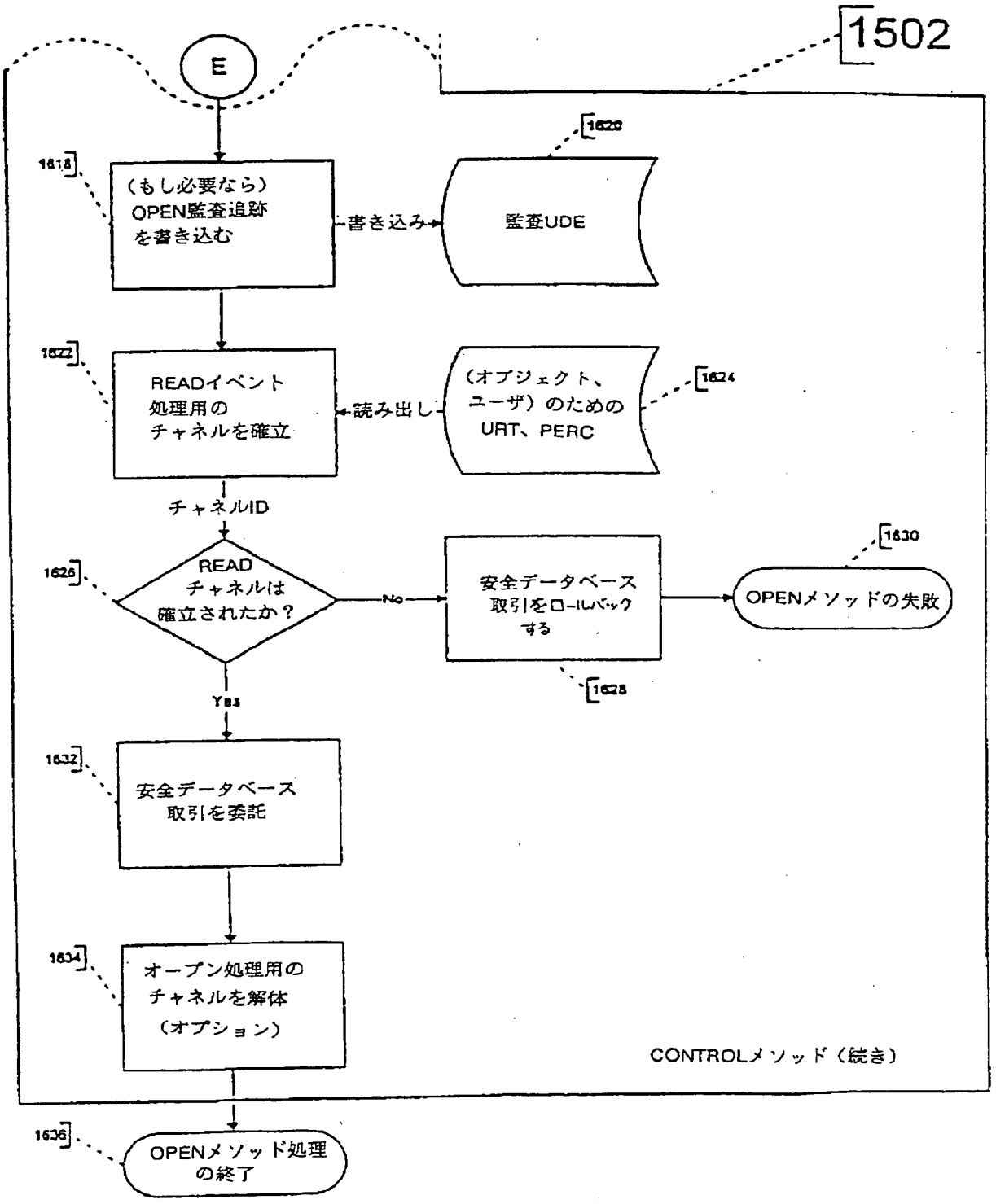


Figure 49f

【図５０】

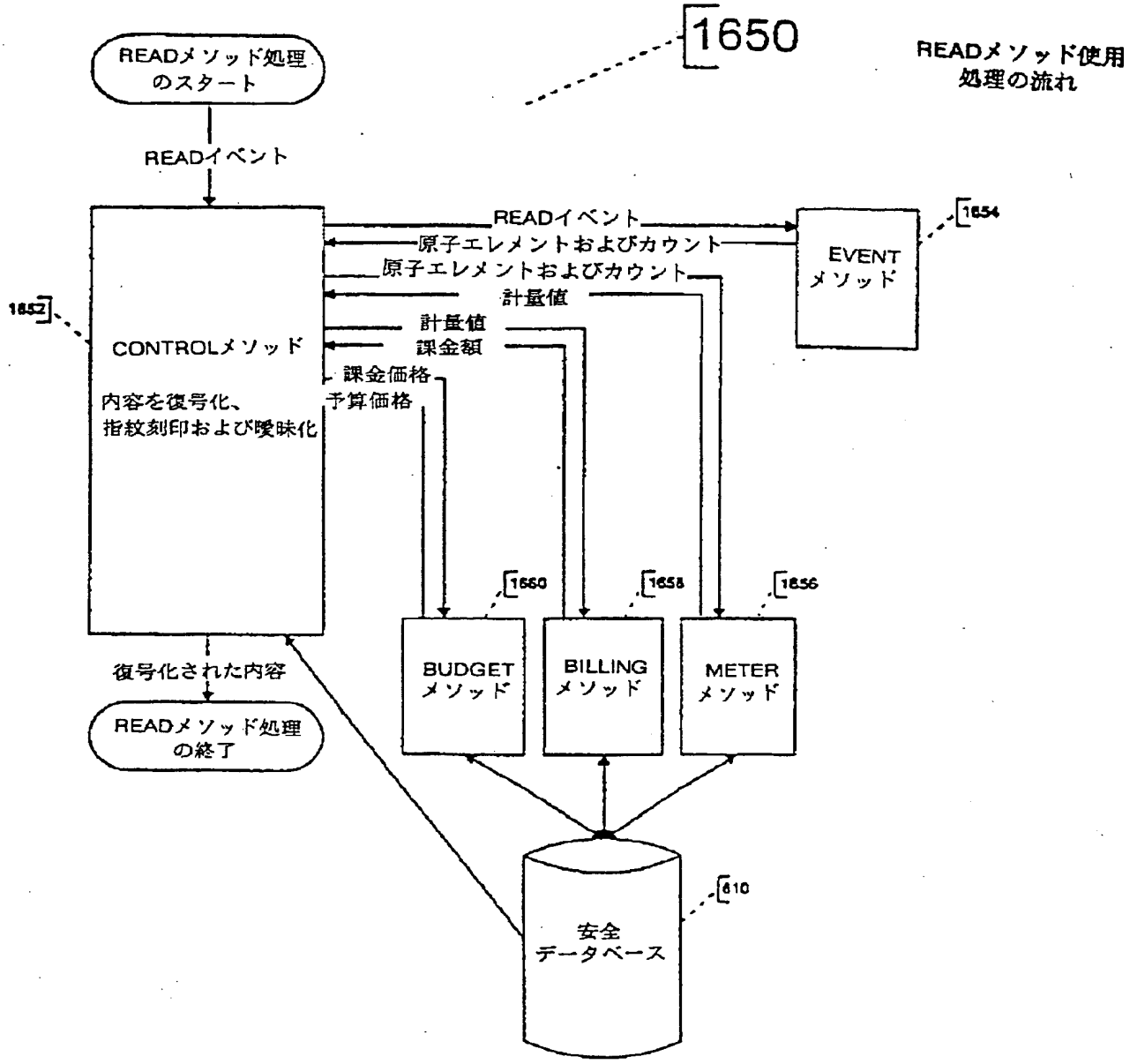


Figure 50

【図５０】

1650

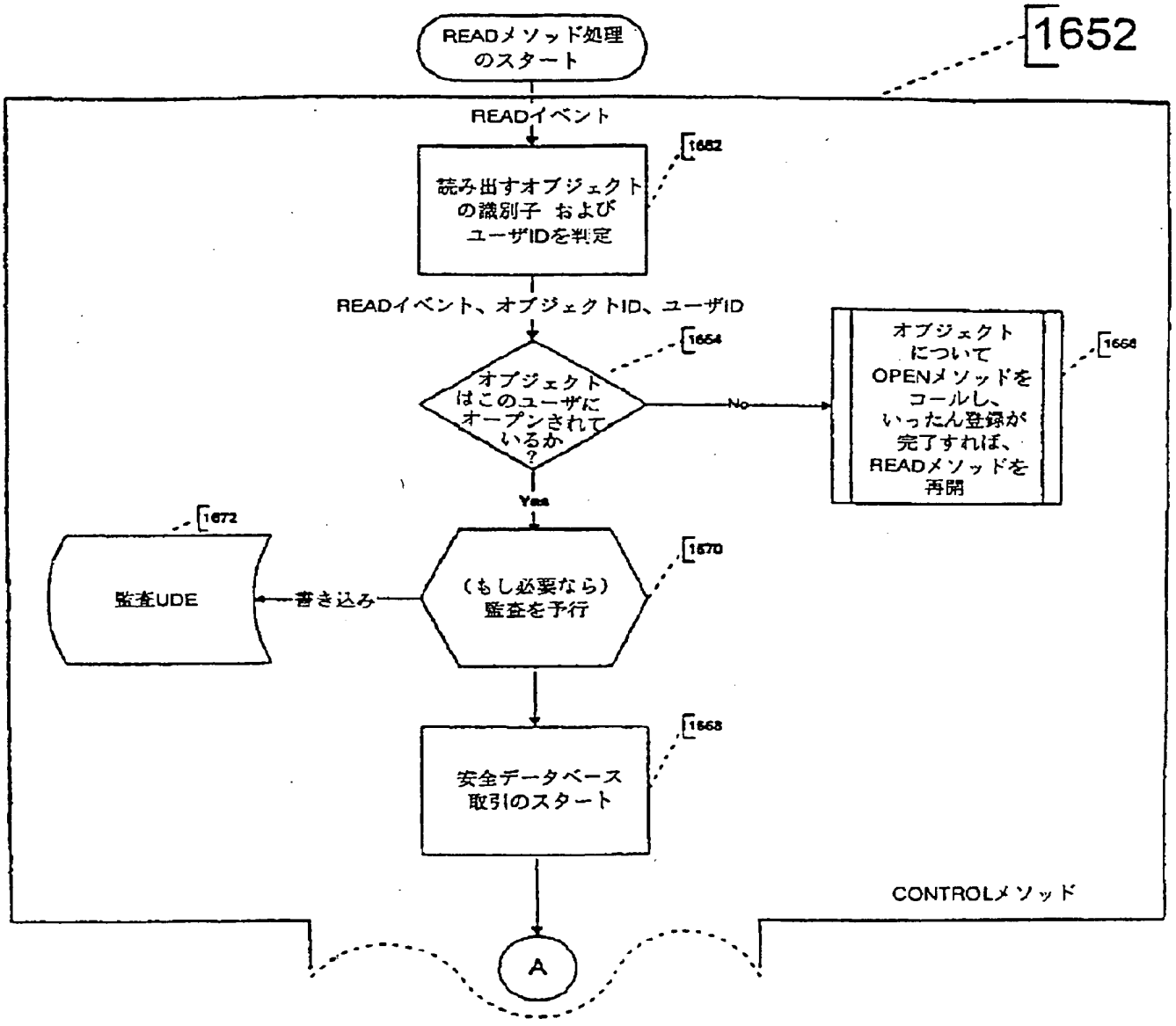


Figure 50a

【図５０】

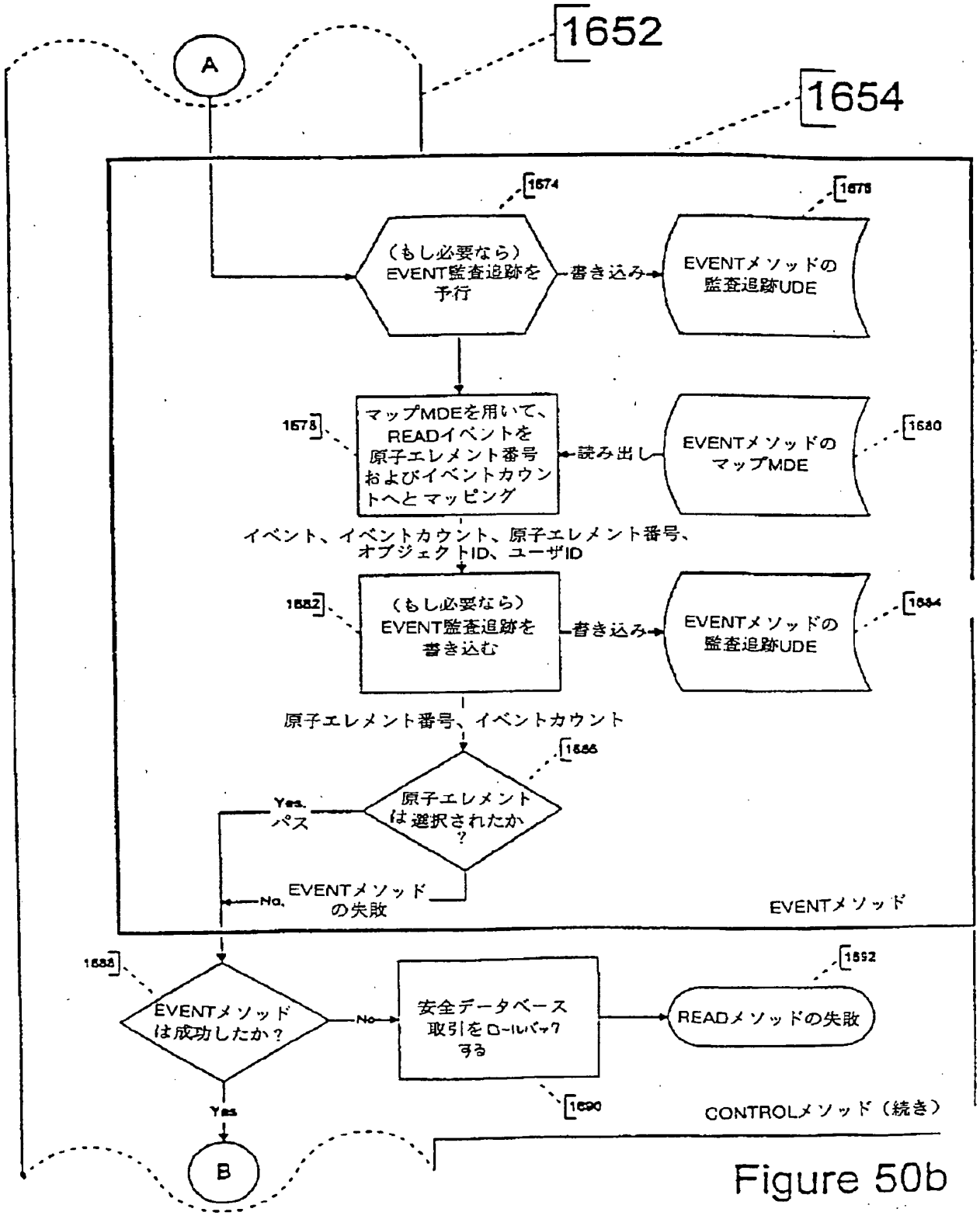


Figure 50b

【図５０】

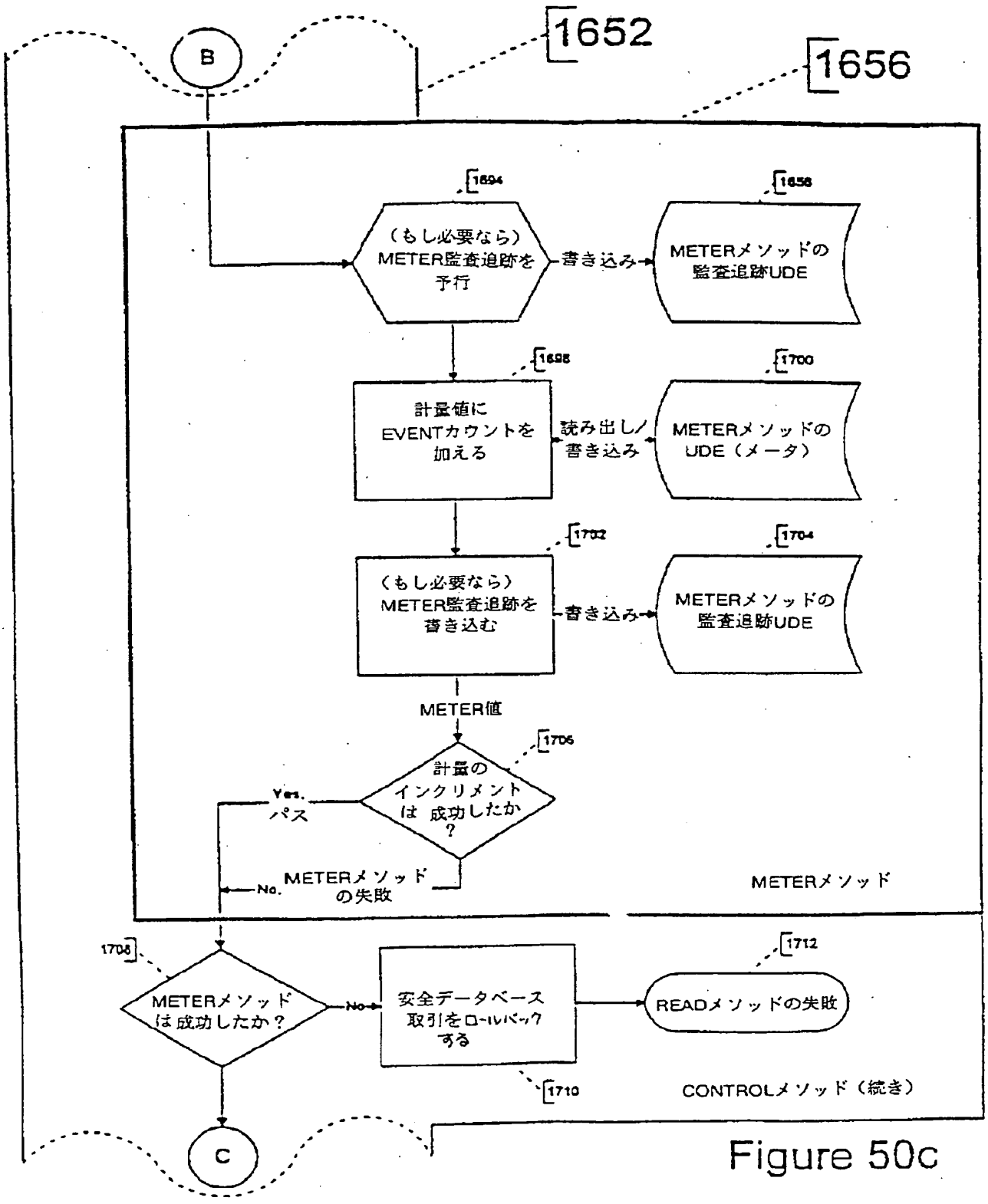


Figure 50c

【図５０】

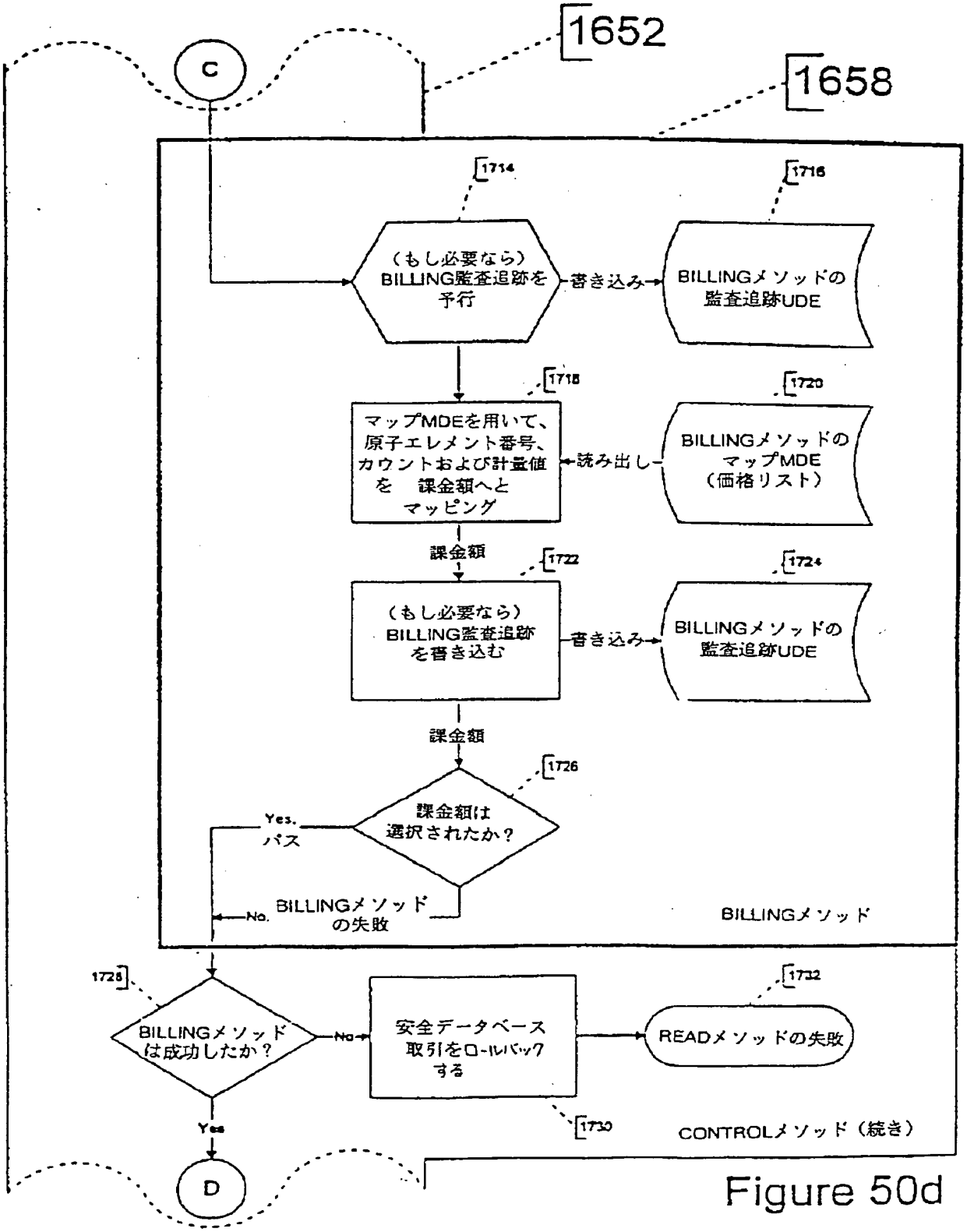


Figure 50d

【図５０】

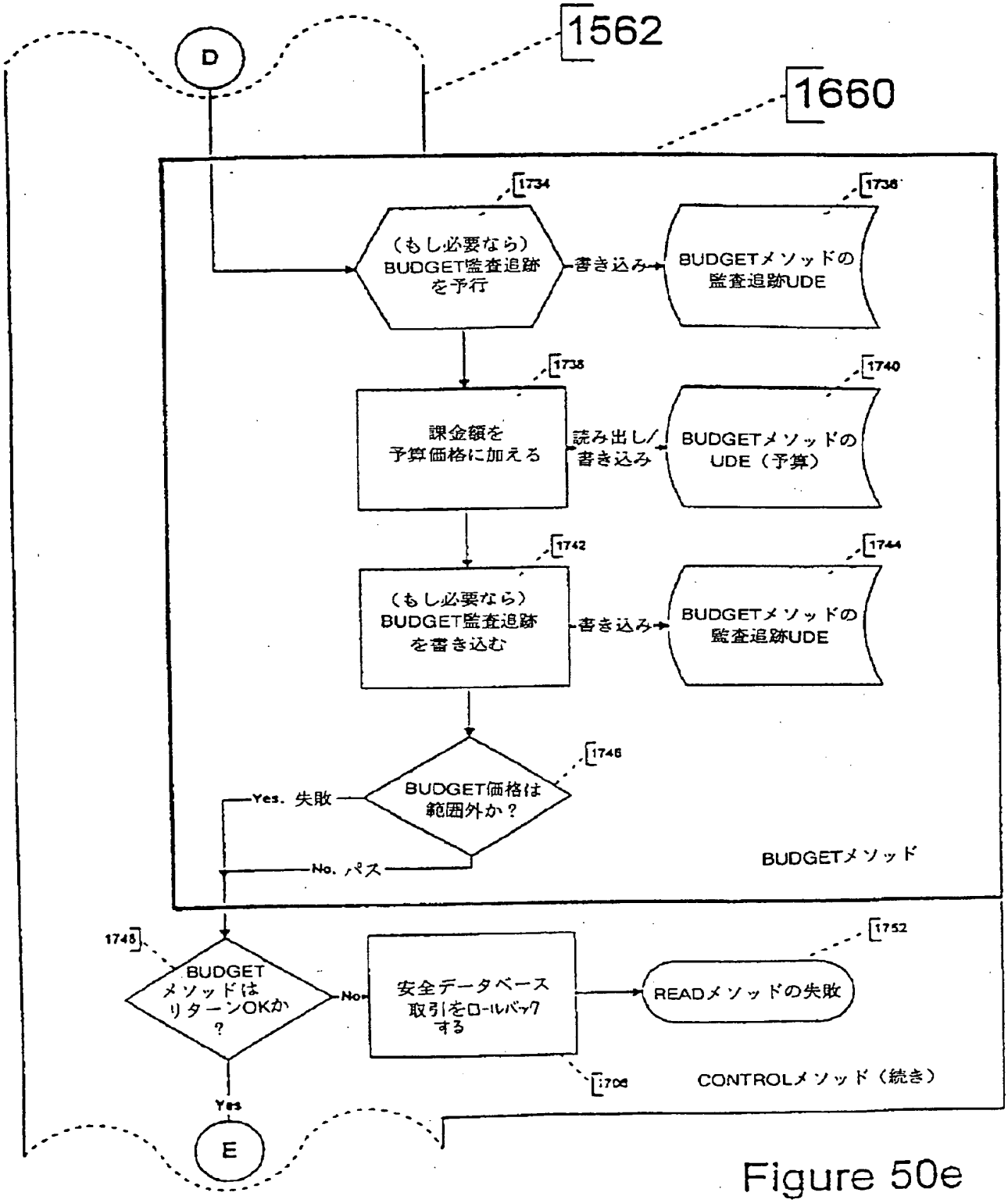
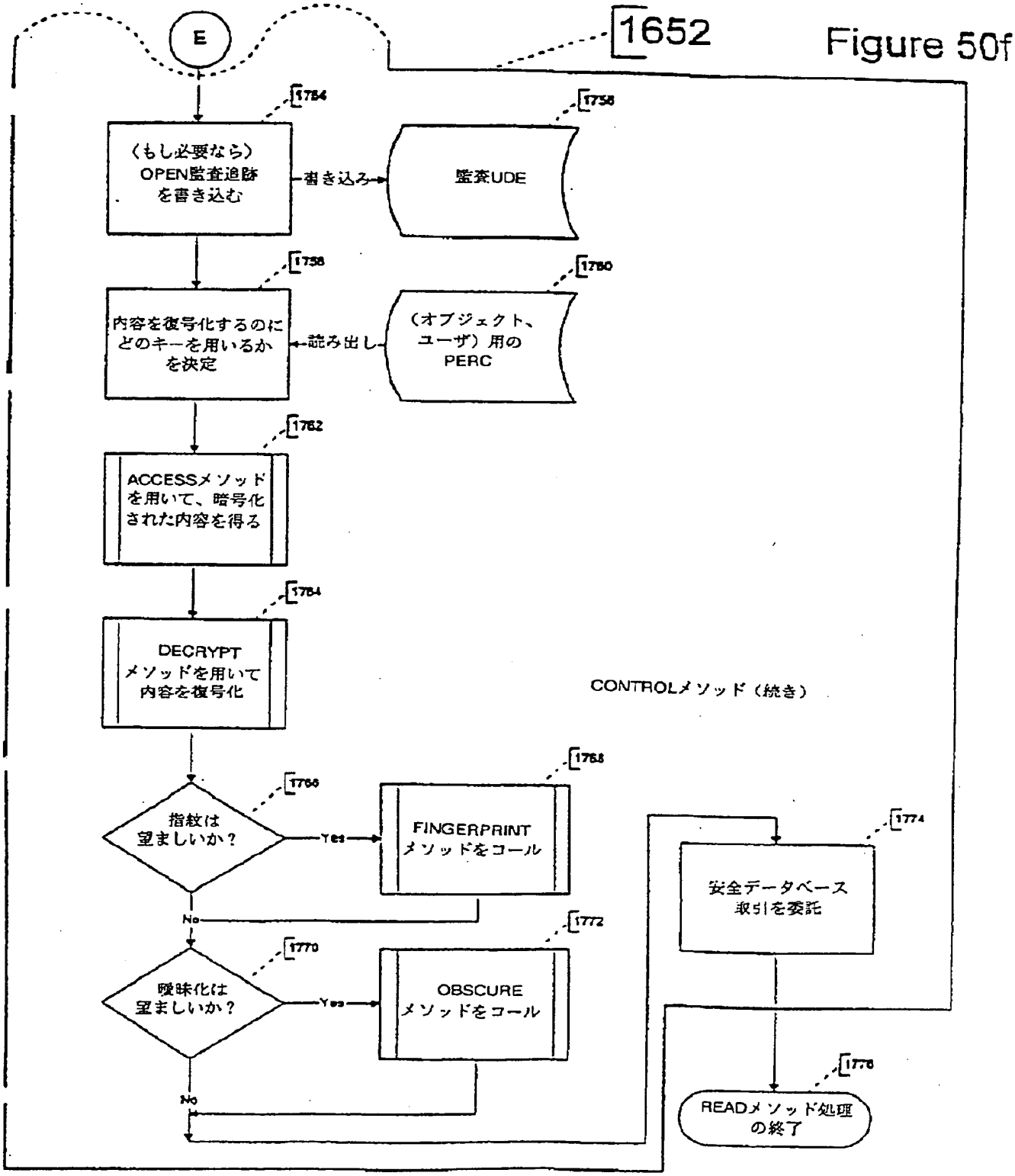


Figure 50e

【図５０】


E
1652
Figure 50f
1754
〈もし必要なら〉
OPEN監査追跡
を書き込む
書き込み
1756
監査UDE
1758
内容を復号化するのに
どのキーを用いるか
を決定
読み出し
1760
（オブジェクト、
ユーザ）用の
PERC
1762
ACCESSメソッド
を用いて、暗号化
された内容を得る
1764
DECRYPT
メソッドを用いて
内容を復号化
CONTROLメソッド（続き）
1766
指紋は
望ましいか？
Yes
1768
FINGERPRINT
メソッドをコール
No
1770
曖昧化は
望ましいか？
Yes
1772
OBSCURE
メソッドをコール
No
1774
安全データベース
取引を委託
1776
READメソッド処理
の終了

【図５１】

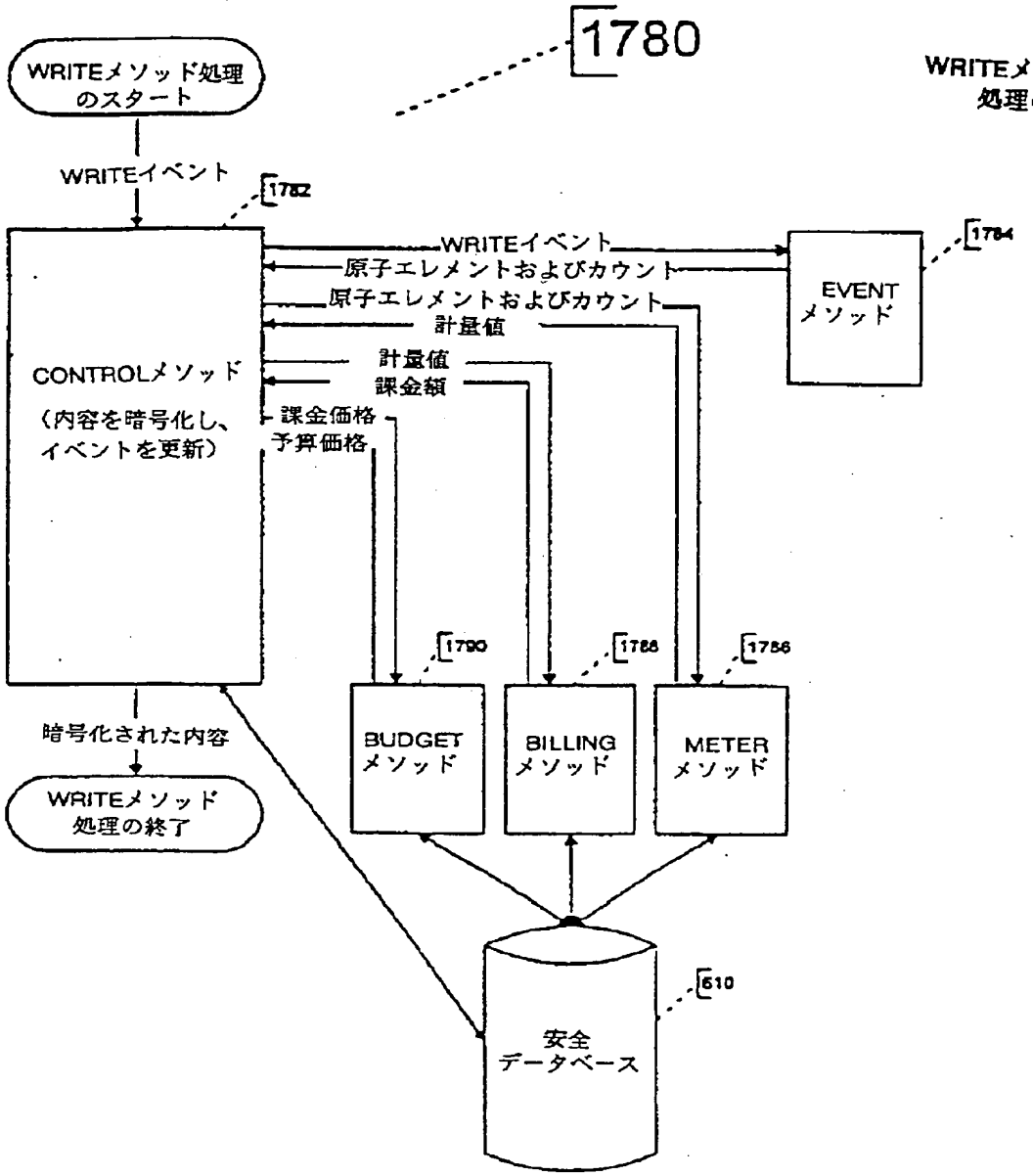


Figure 51

【図５１】

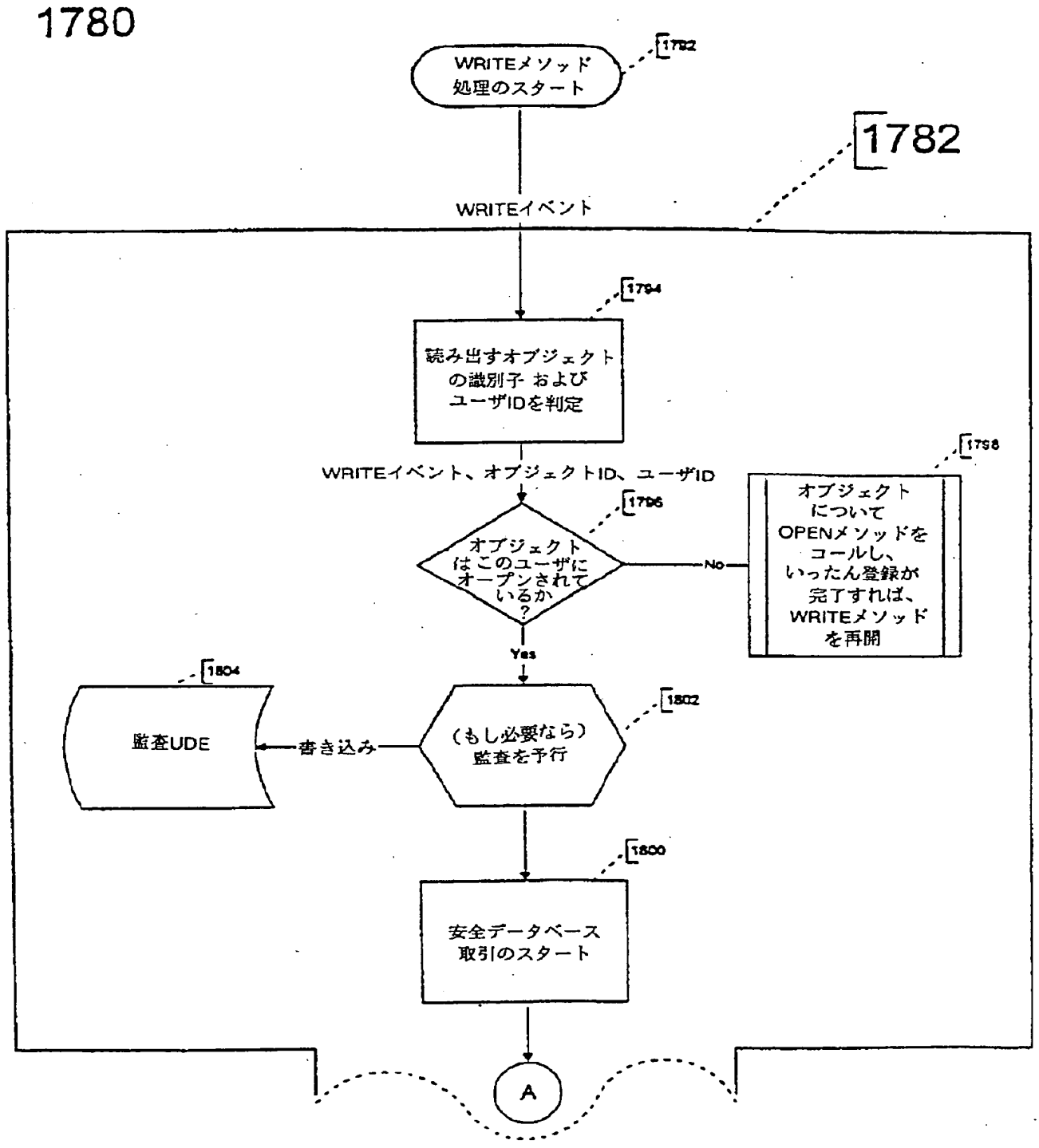


Figure 51a

【図５１】

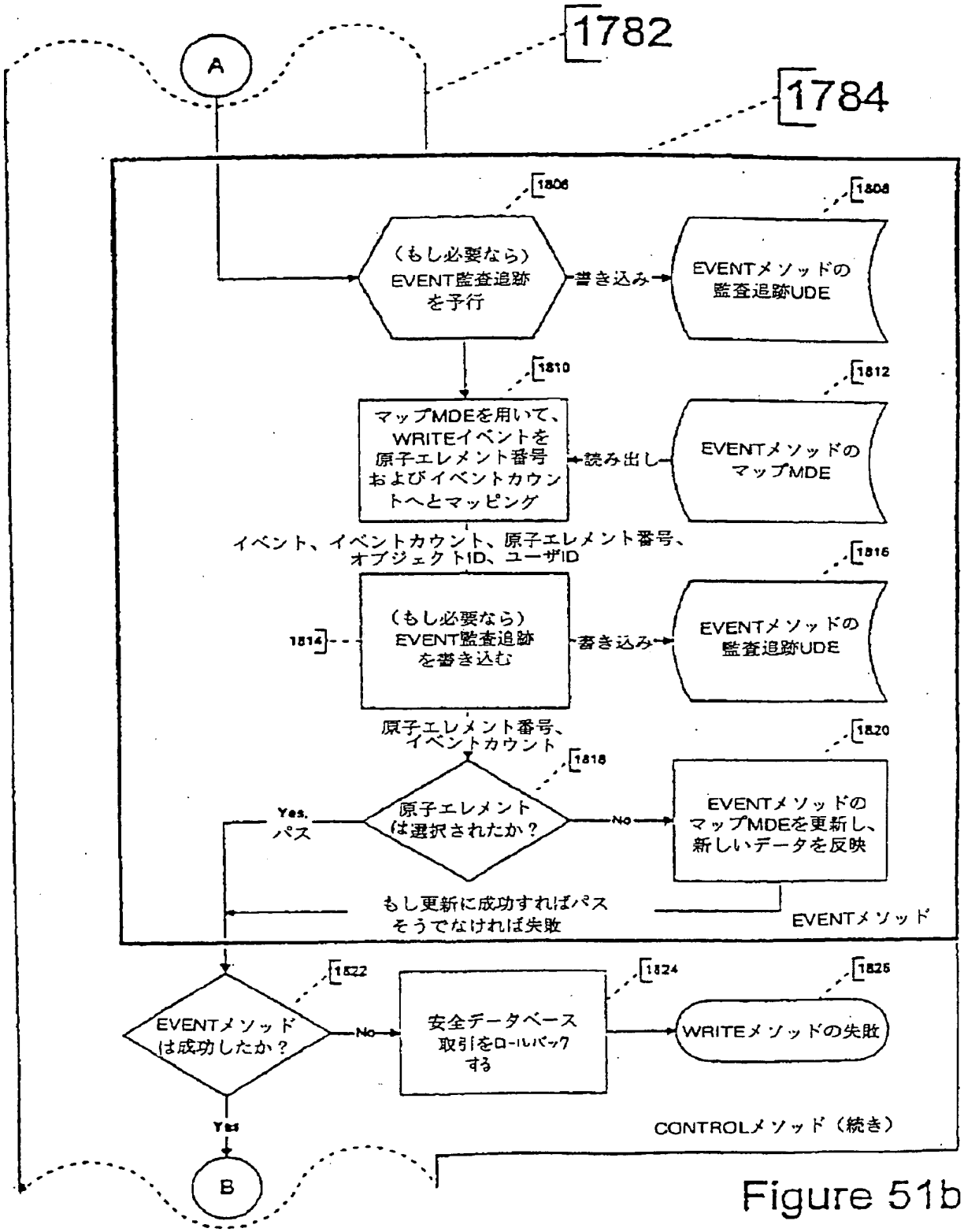


Figure 51b

【図５１】

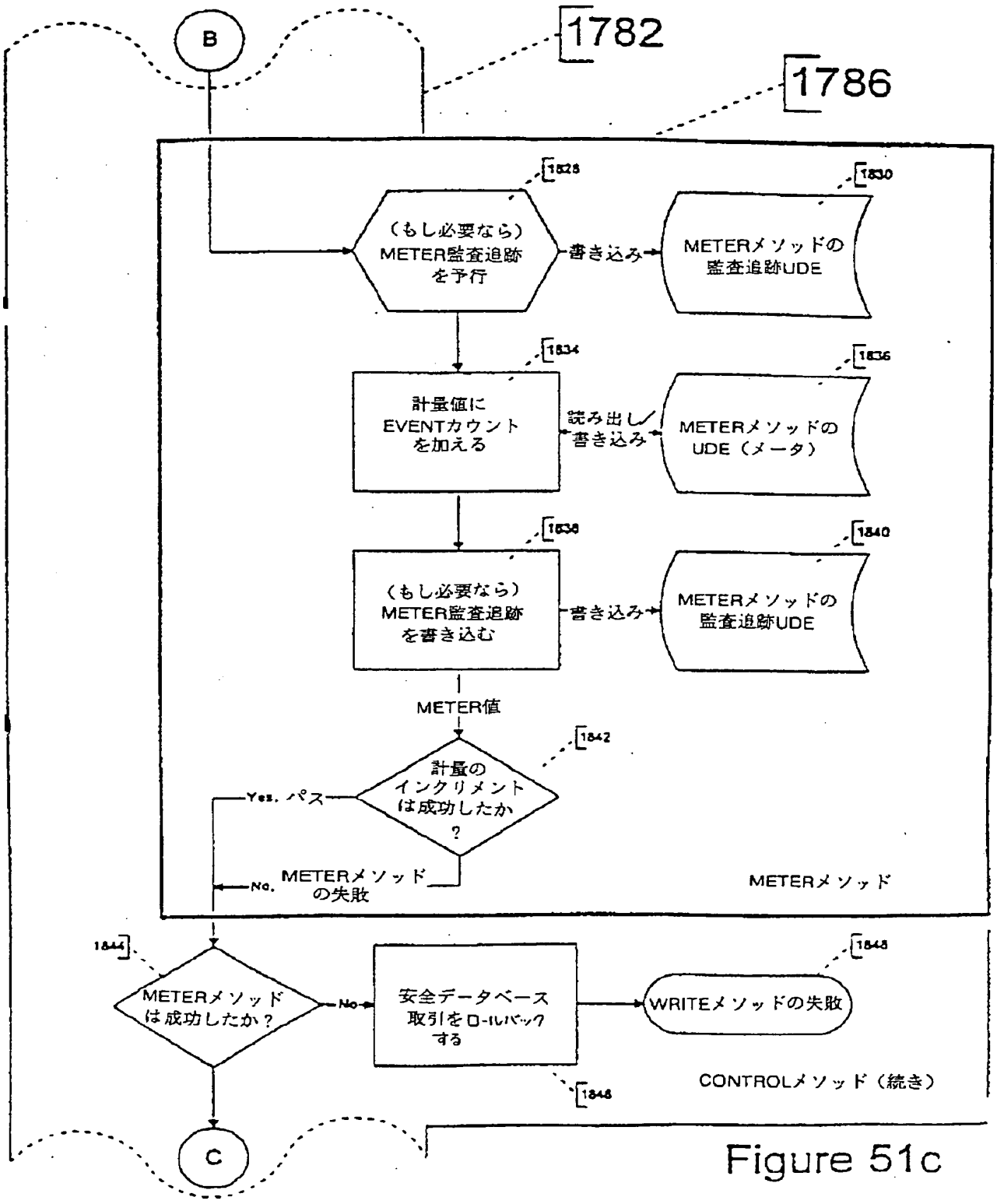


Figure 51c

【図５１】

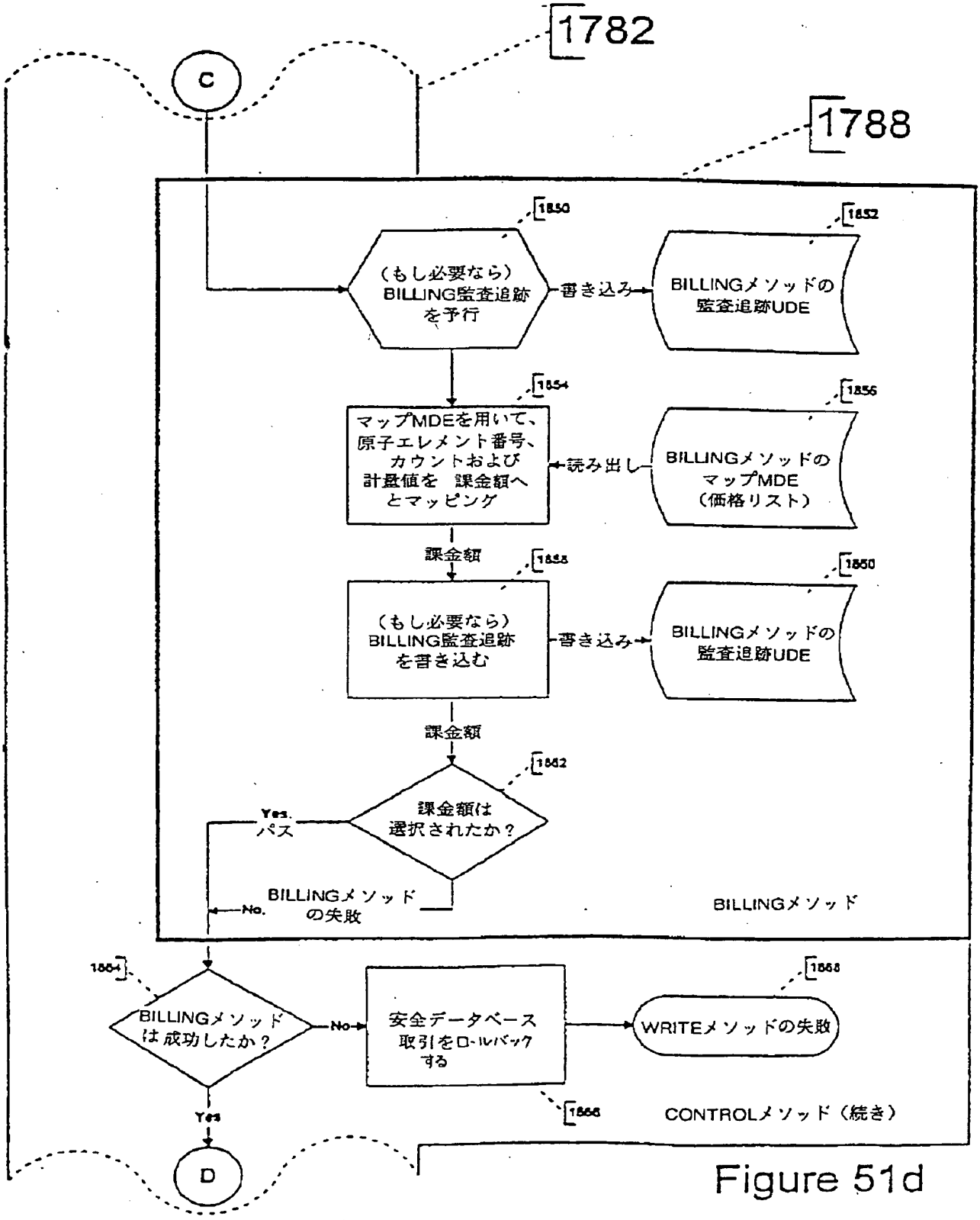


Figure 51d

【図５１】

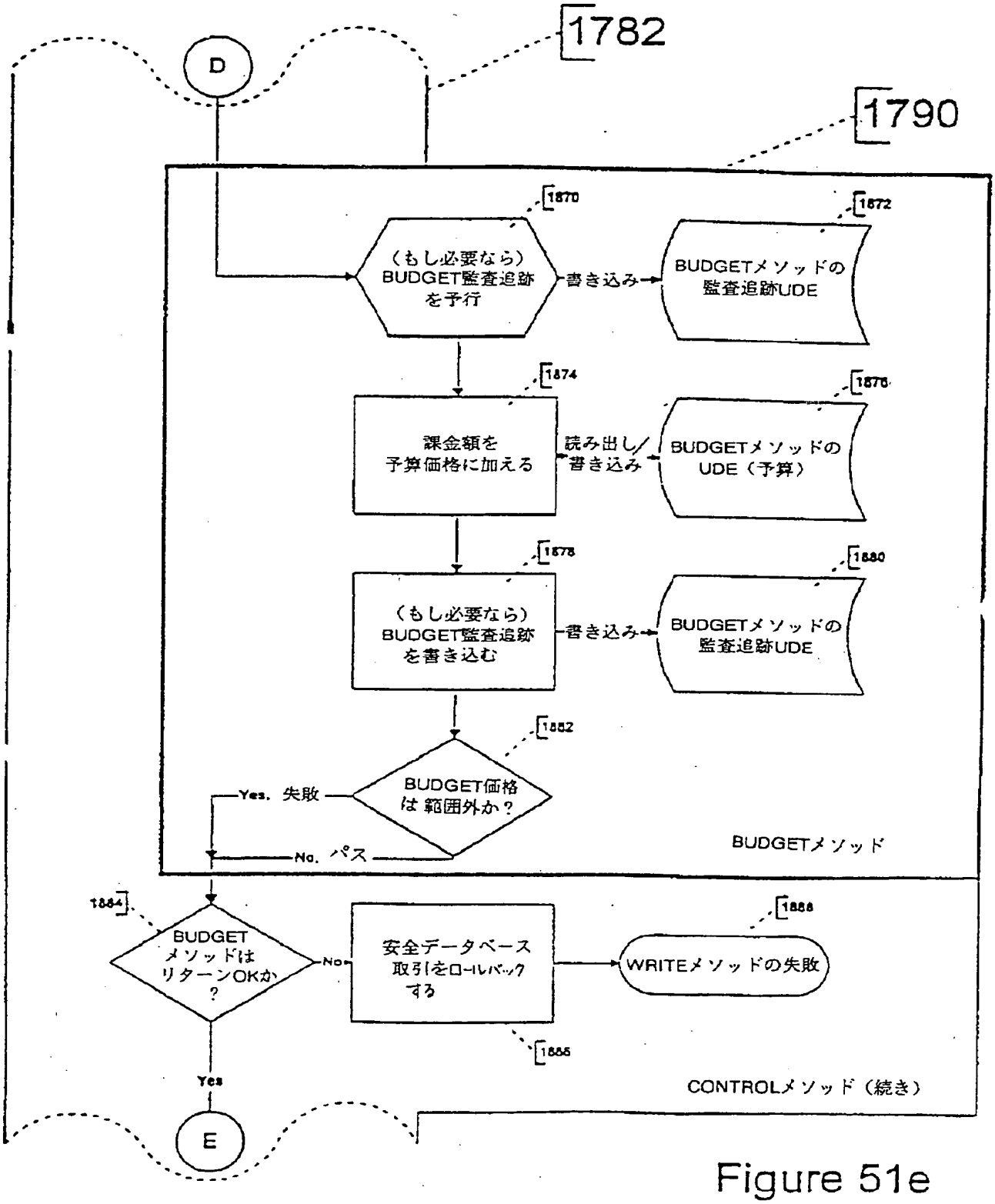


Figure 51e

【図５１】

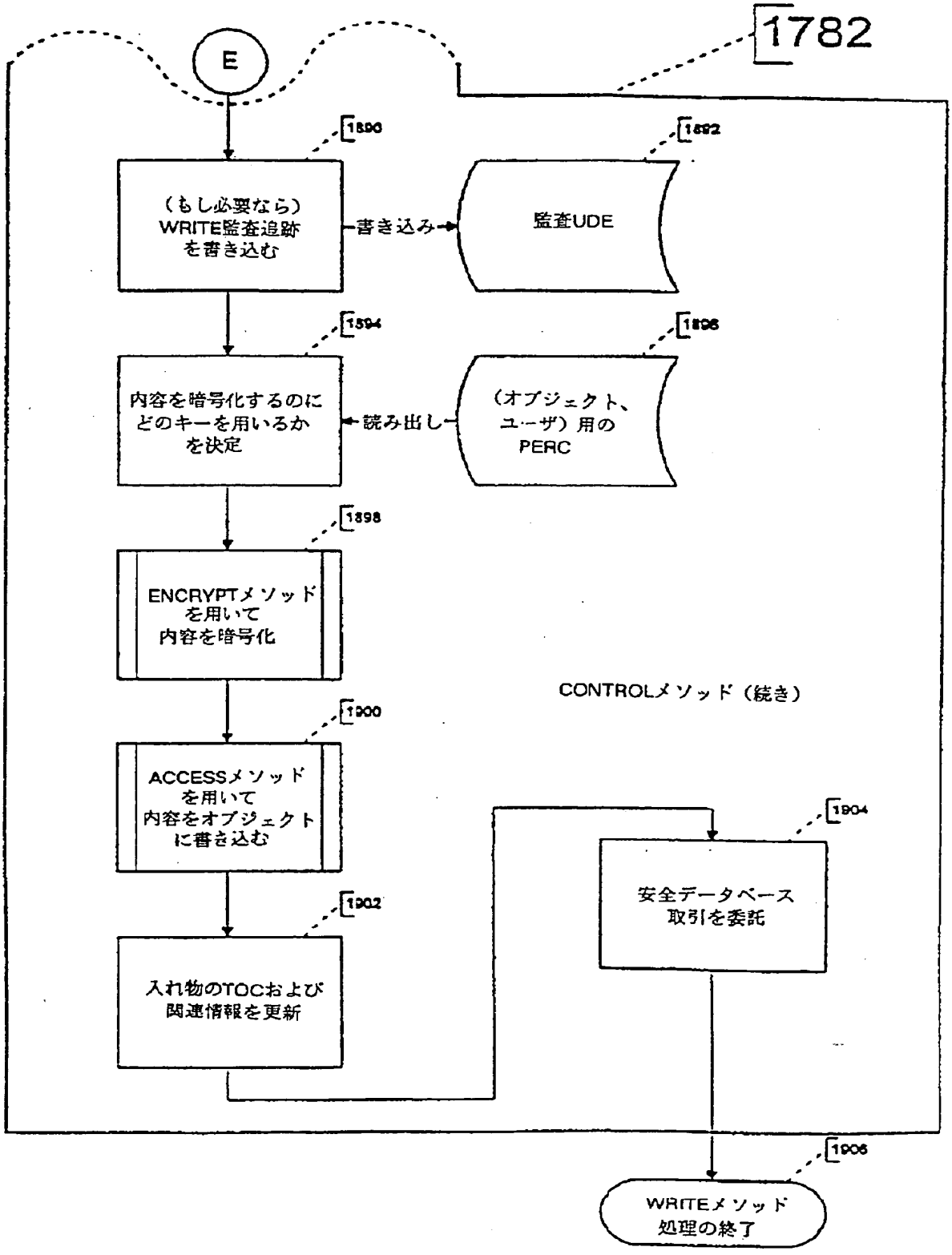
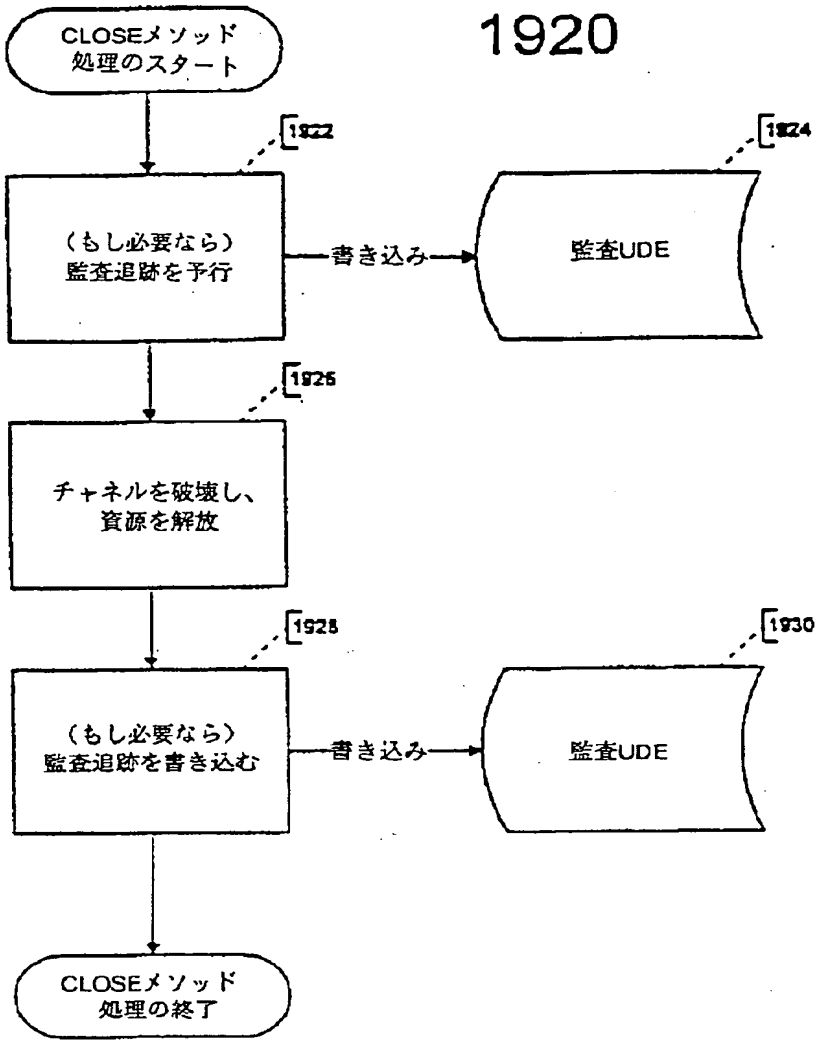


Figure 51f

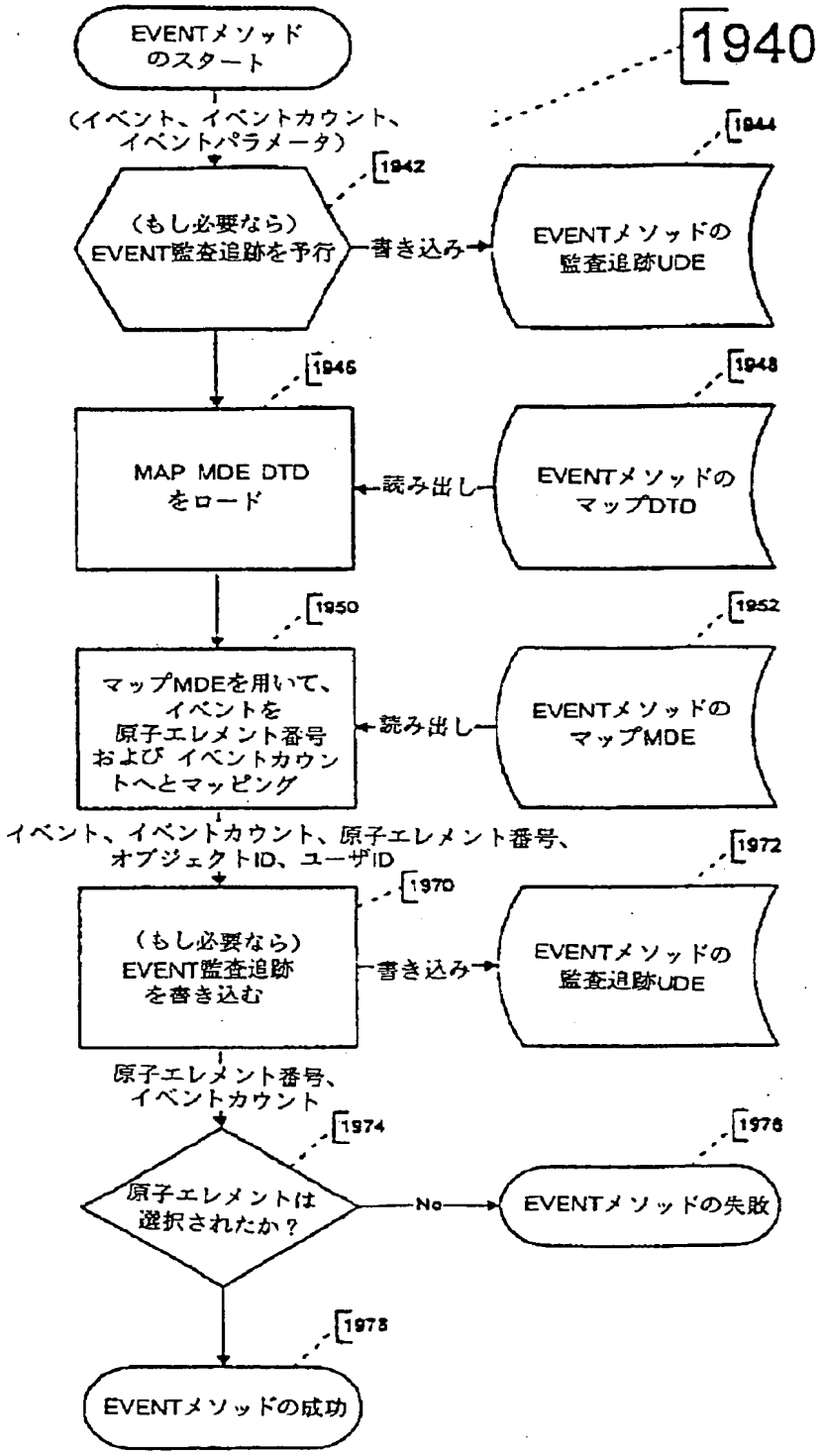
【図５２】



CLOSEメソッド
処理の流れ

Figure 52

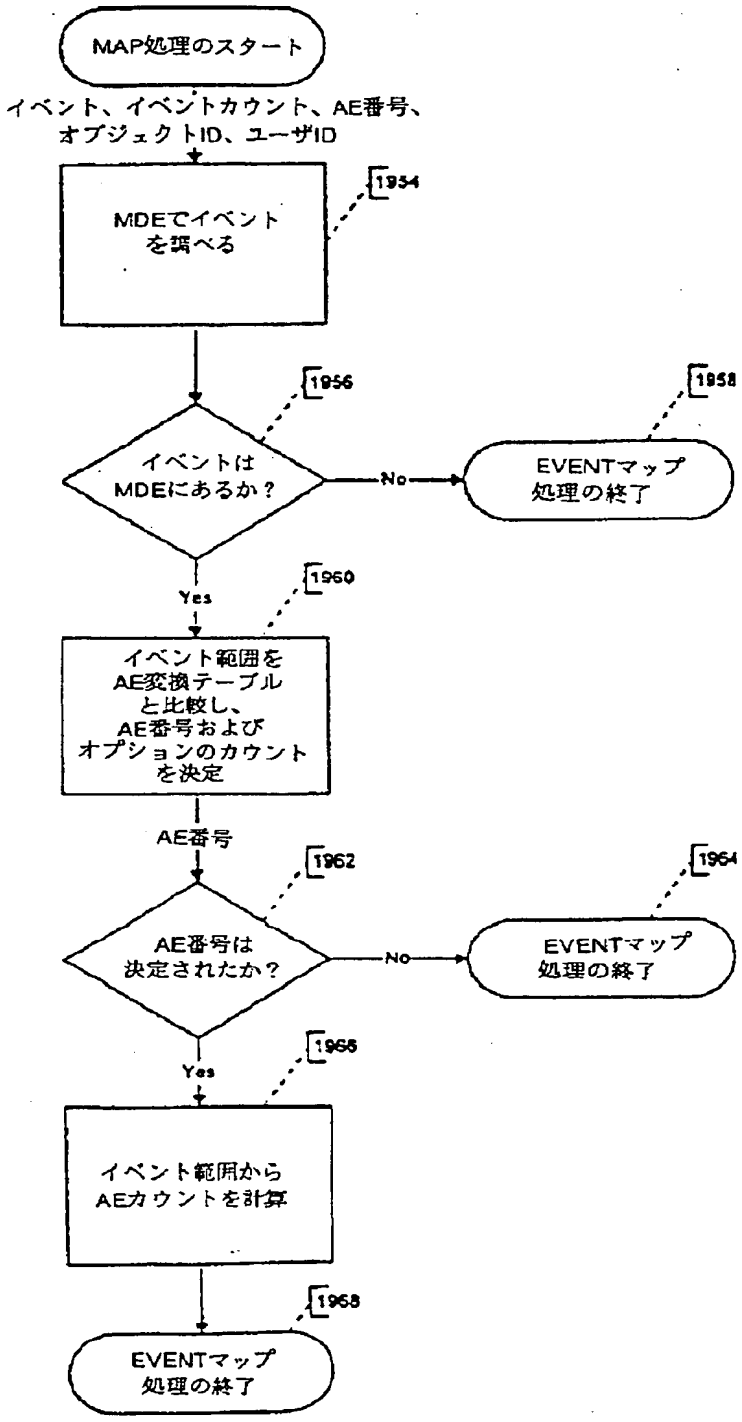
【図５３】



EVENTメソッド
処理の流れ

Figure 53a

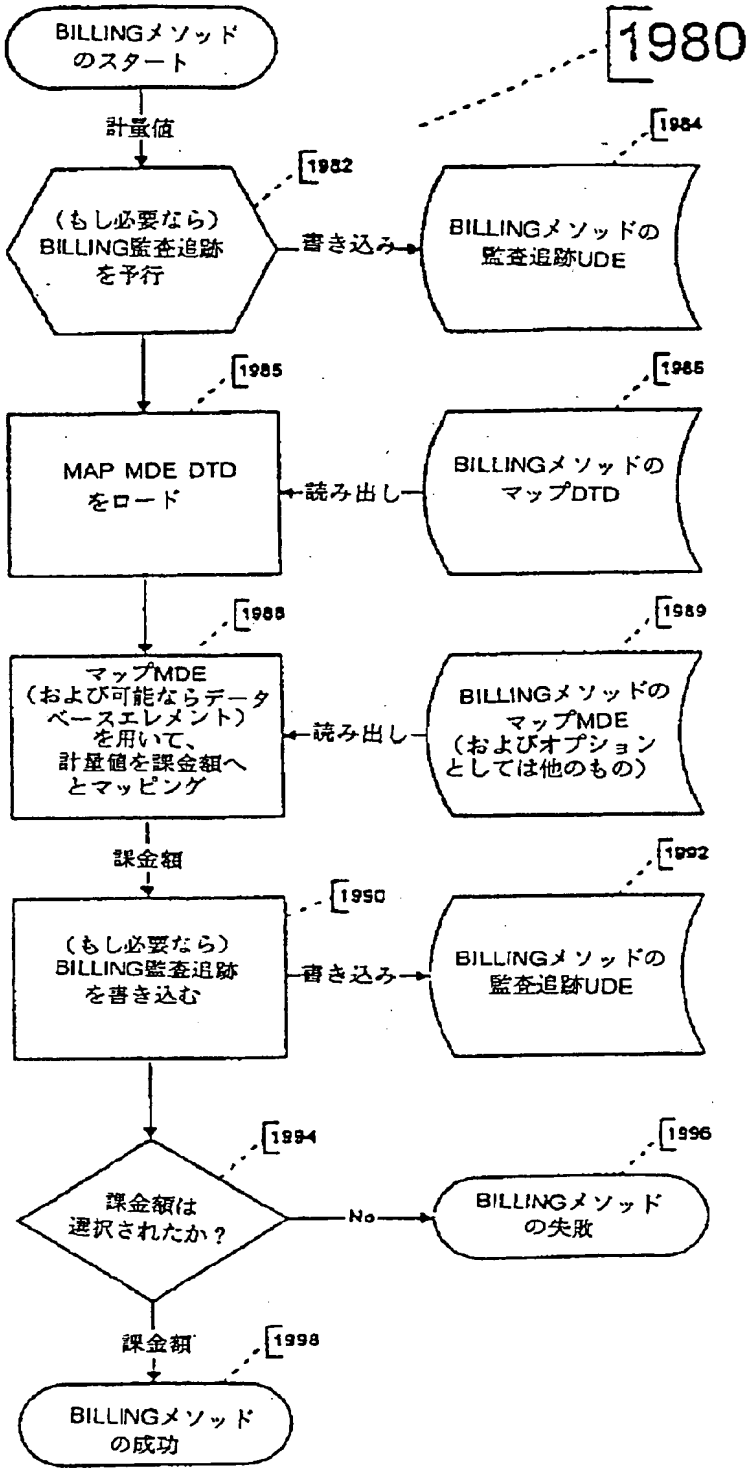
【図５３】



EVENTメソッド
マッピング処理のサンプル

Figure 53b

【図５３】



BILLINGメソッド
処理の流れ

Figure 53c

【図５４】

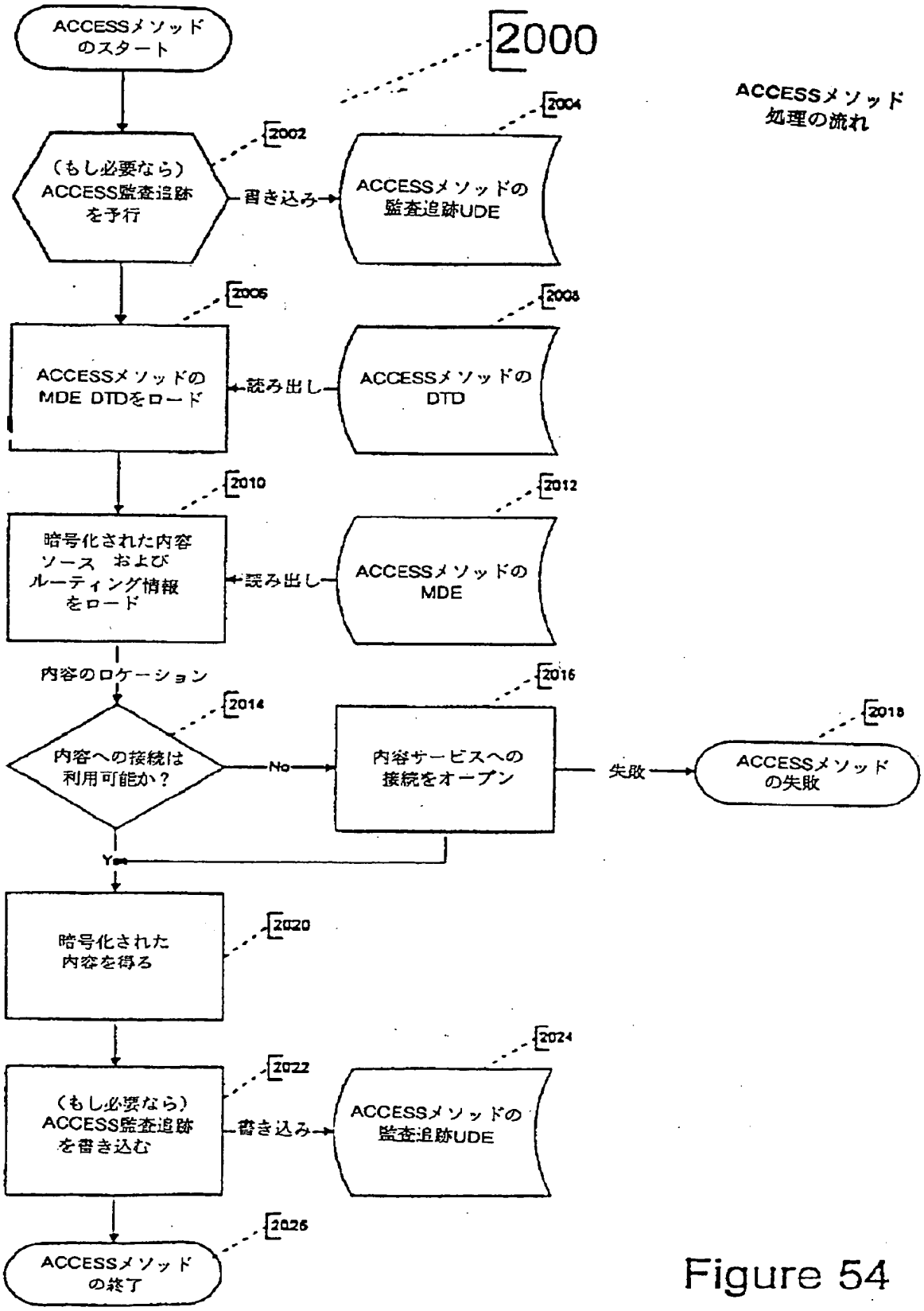


Figure 54

【図５５】

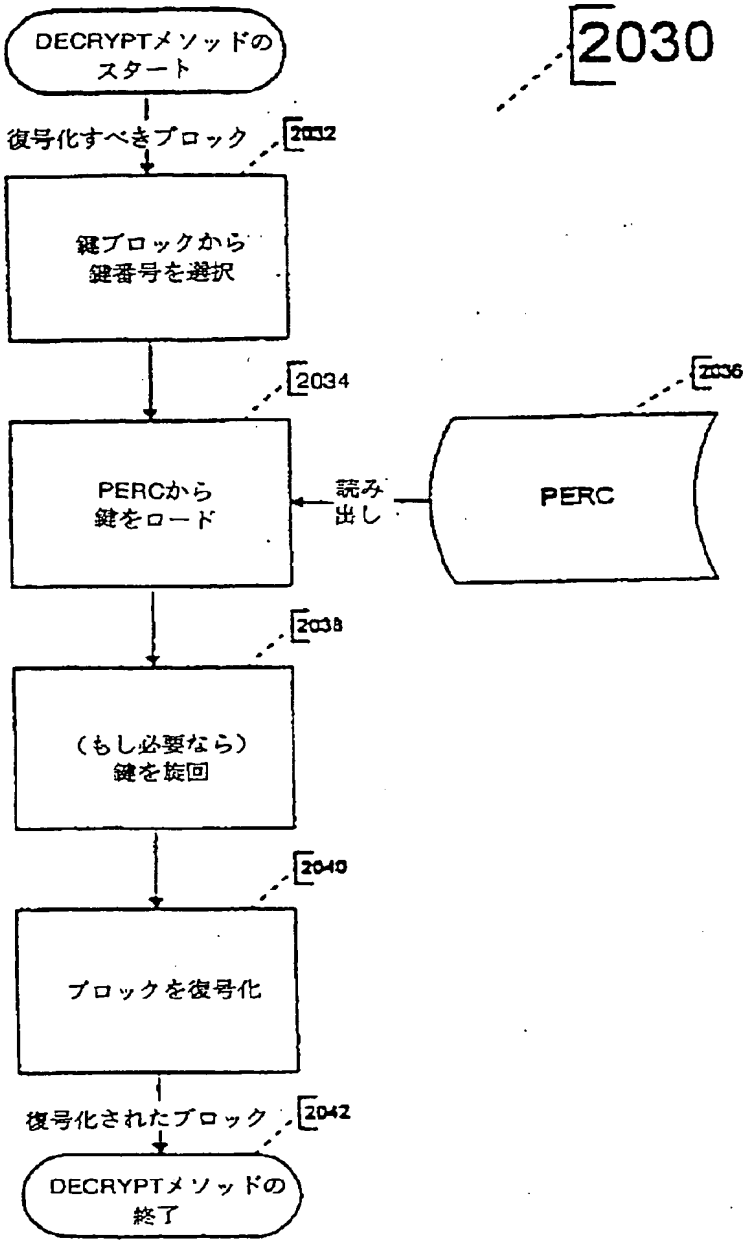


Figure 55a

【図５５】

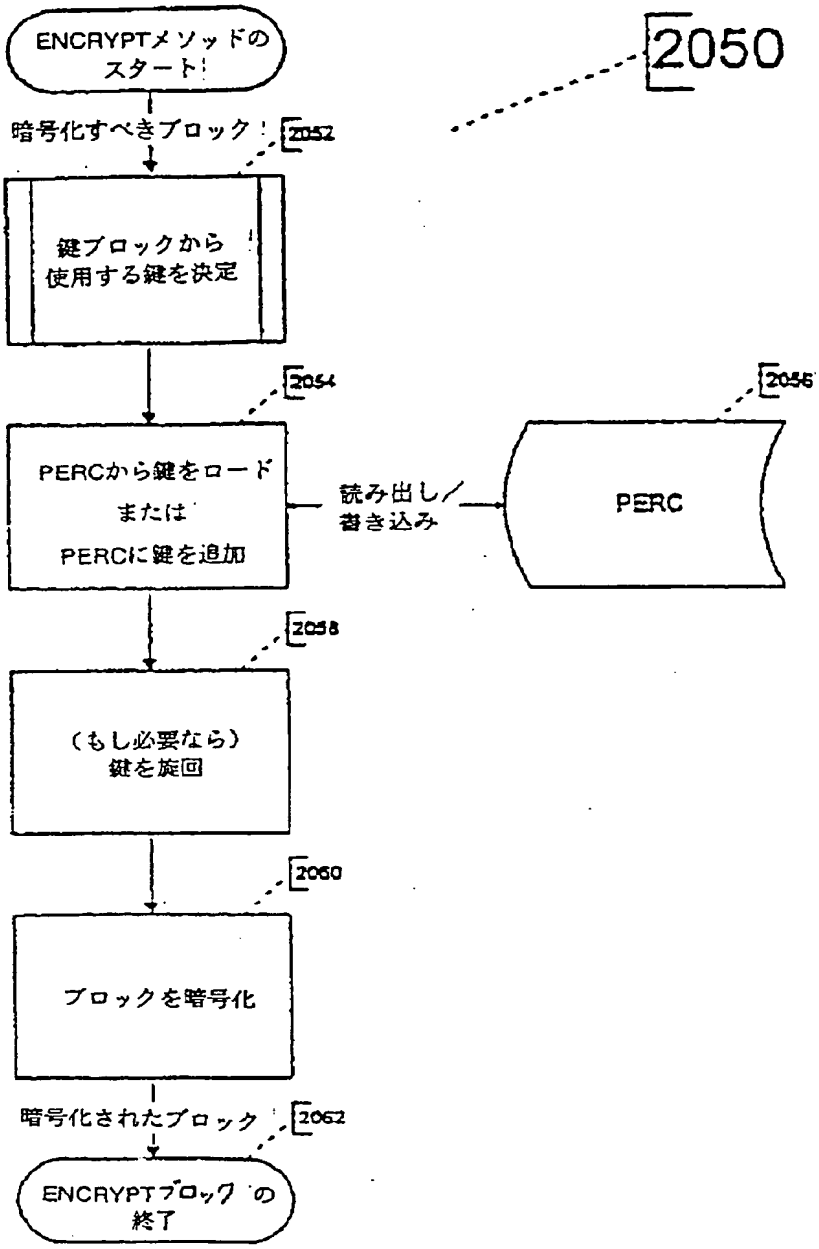
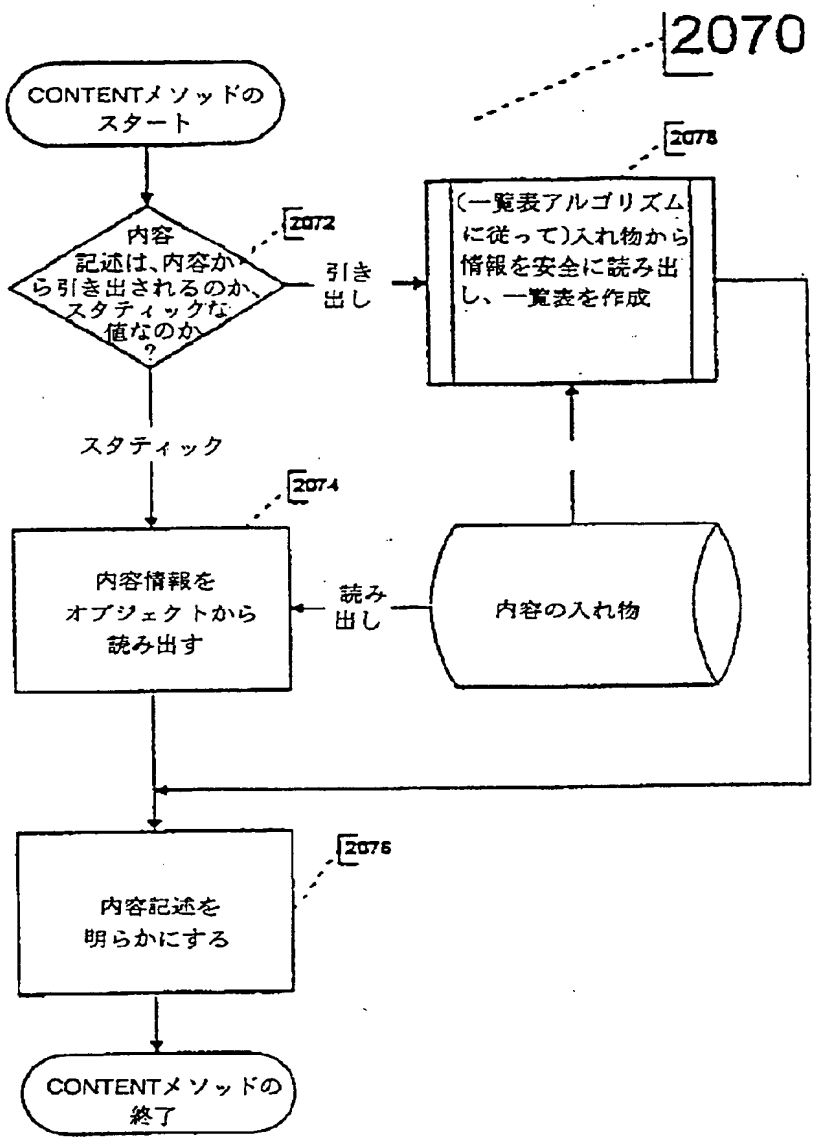


Figure 55b

【図５６】



CONTENTメソッド
処理の流れ

Figure 56

【図５７】

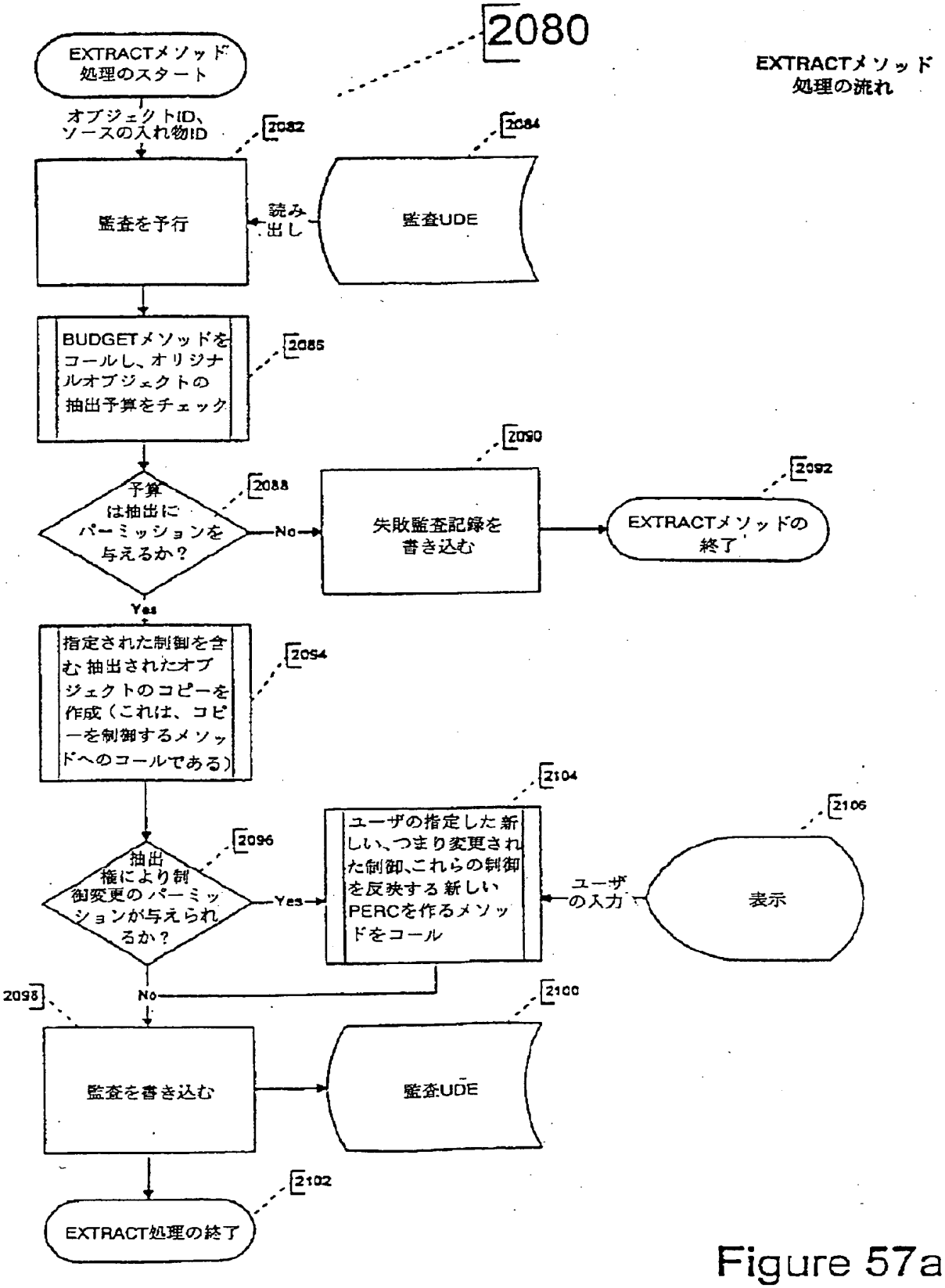


Figure 57a

【図５７】

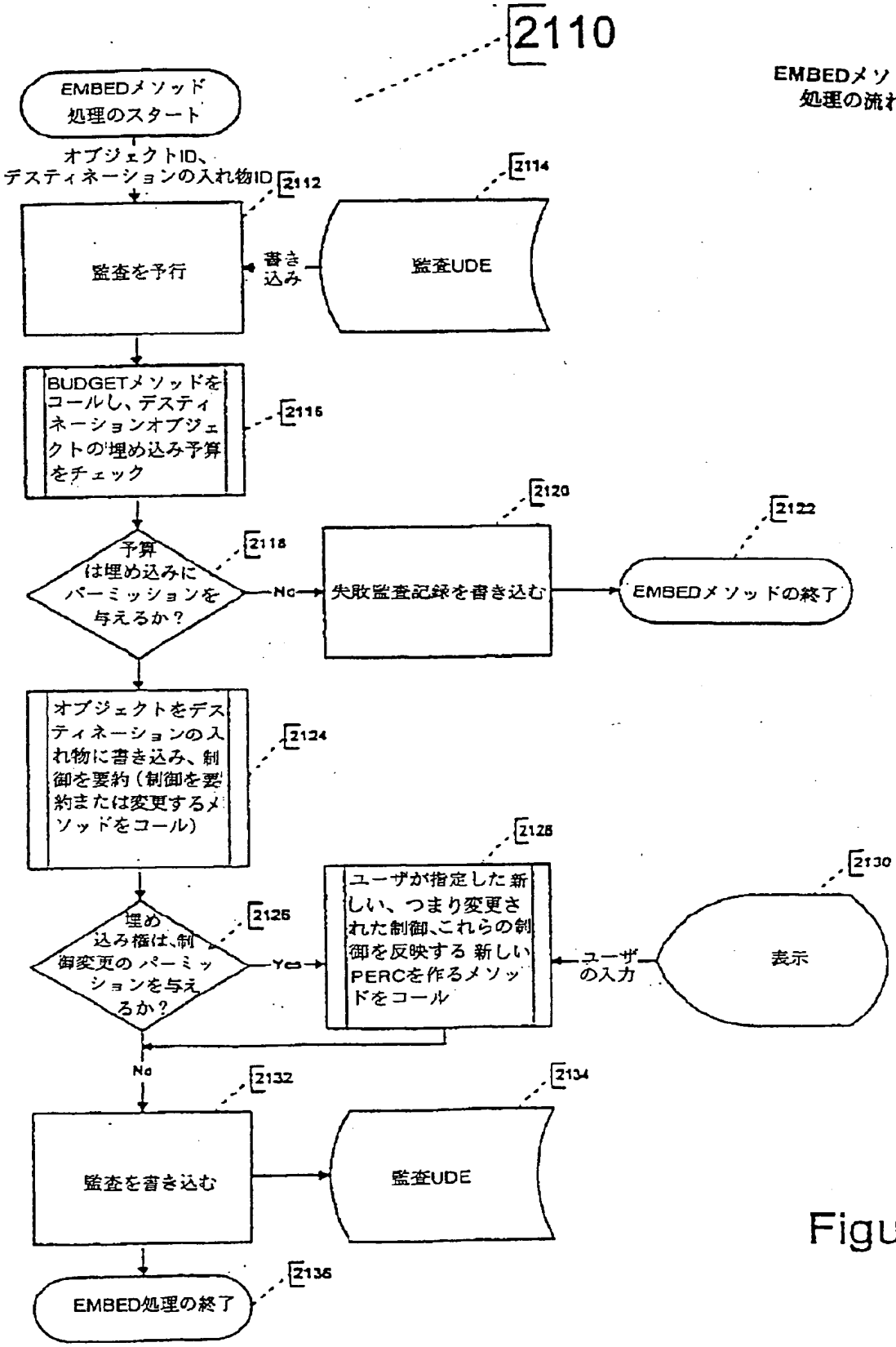


Figure 57b

【図５８】

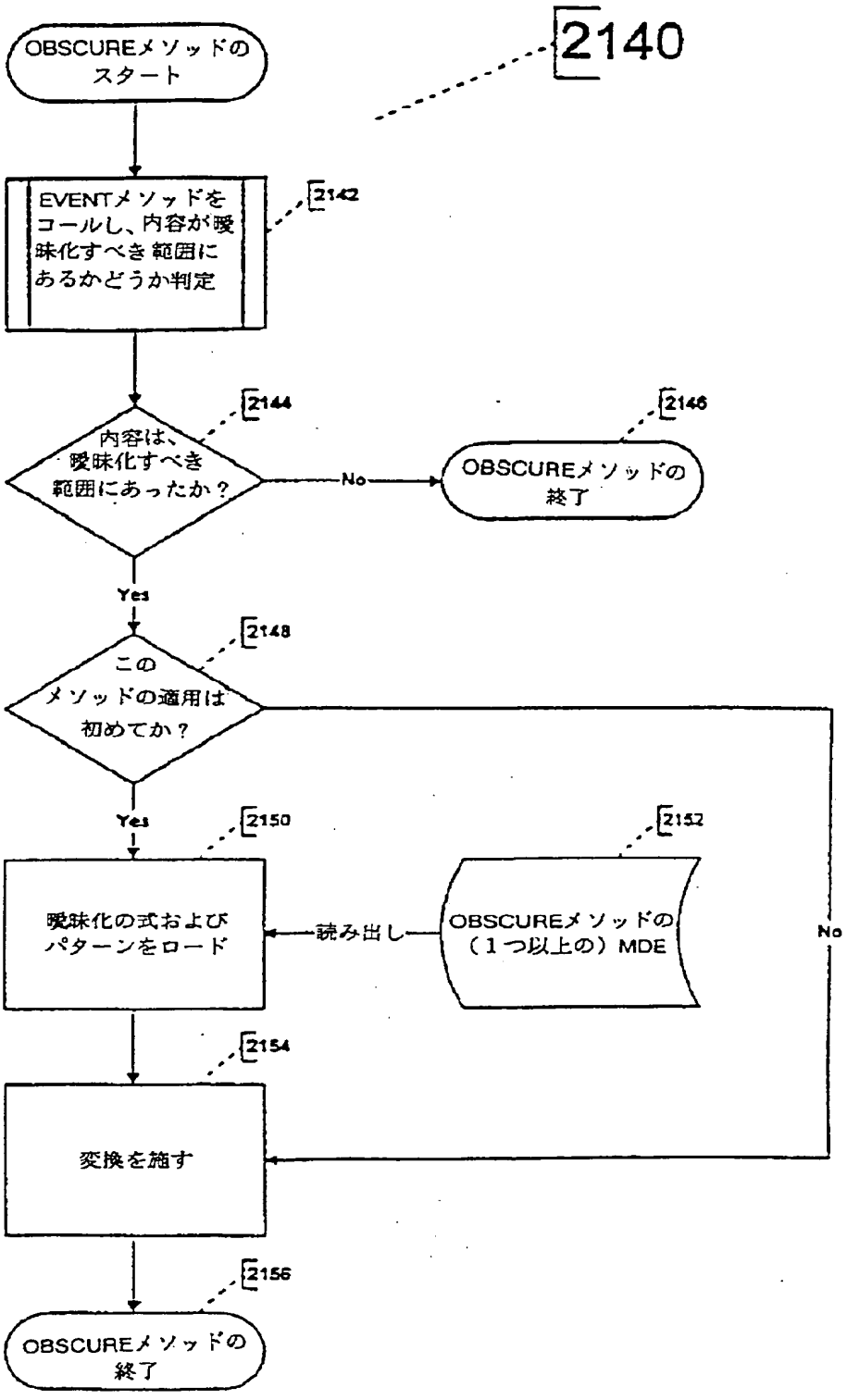
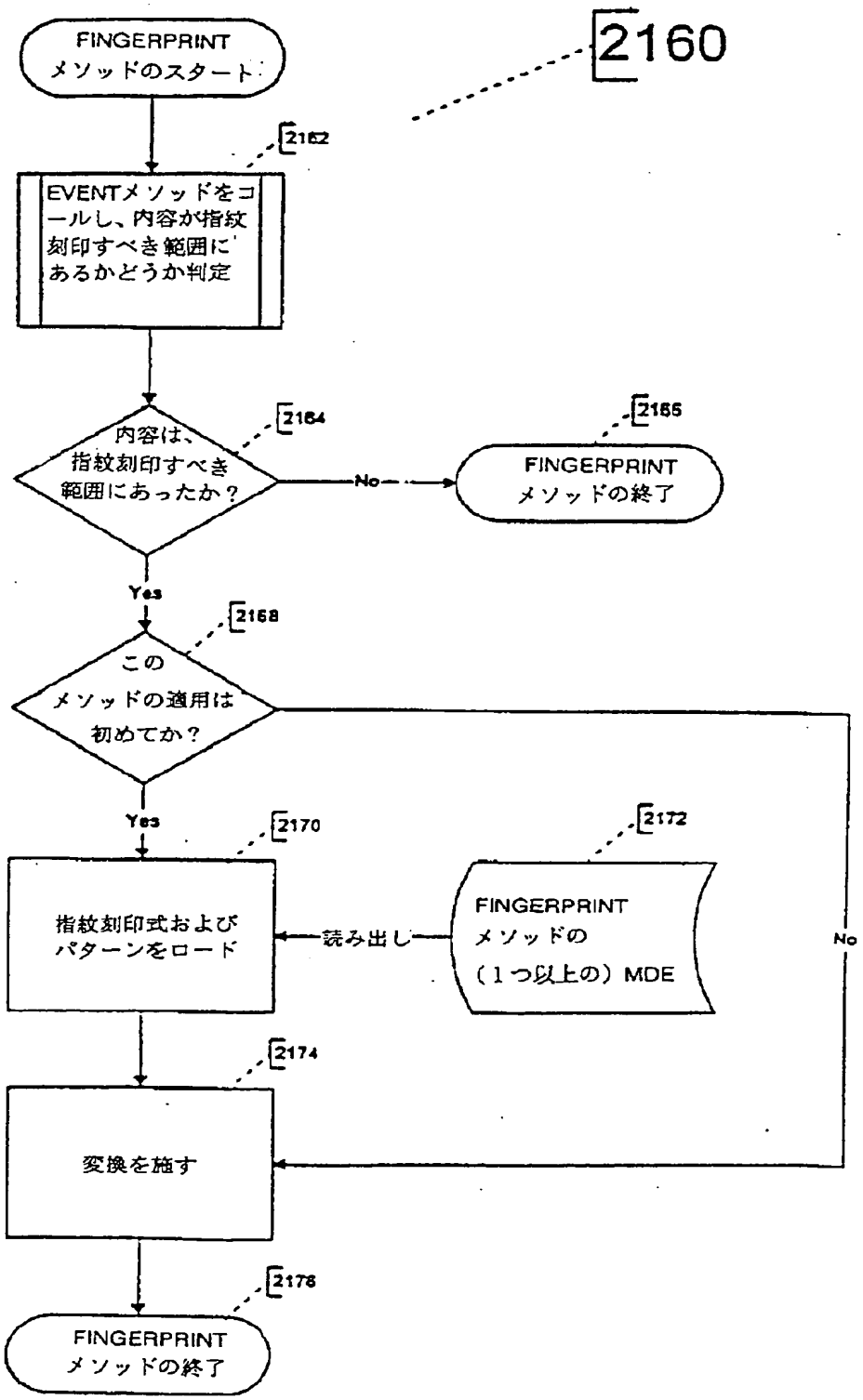


Figure 58a

【図５８】



FINGERPRINTメソッド処理の流れ

Figure 58b

【図５８】

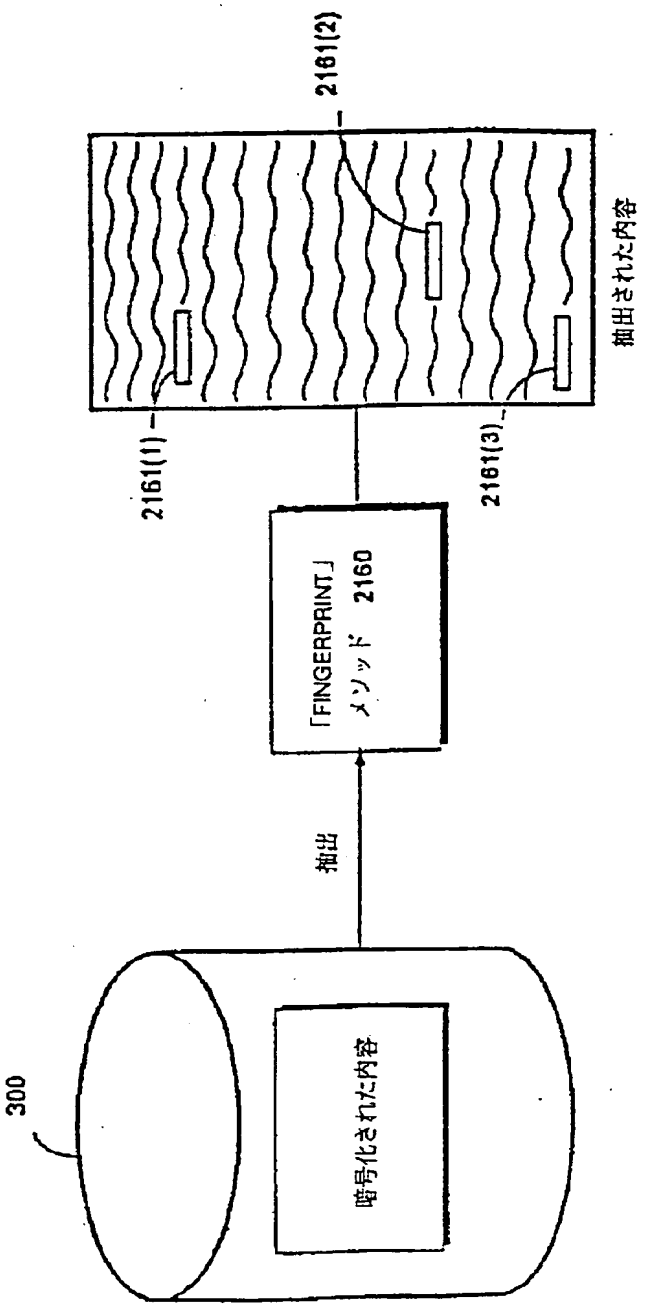
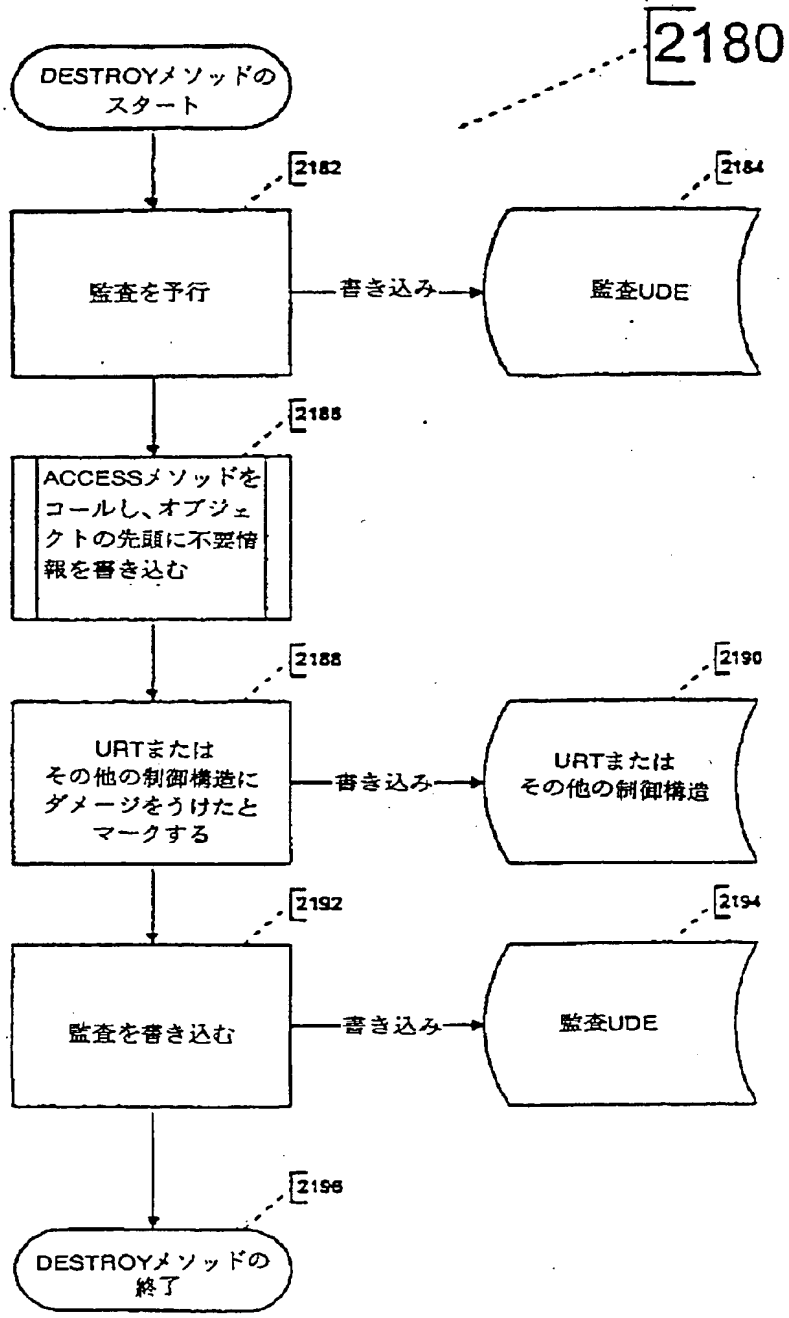

2161(2)
抽出された内容
2161(1)
2161(3)
「FINGERPRINT」
メソッド 2160
抽出
300
暗号化された内容

FIG. 58C

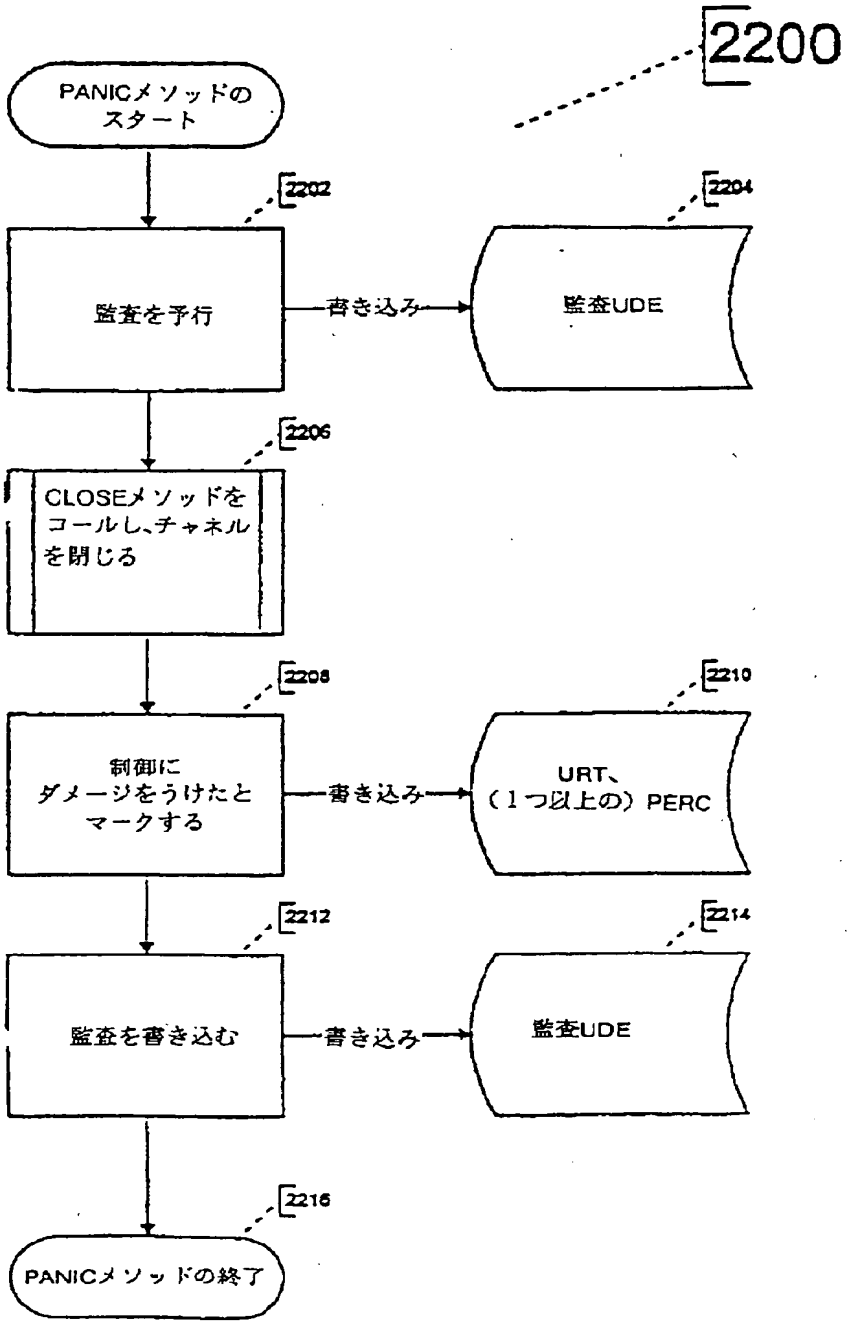
【図５９】



DESTROYメソッド
処理の流れ

Figure 59

［図６０］



PANICメソッド
処理の流れ

Figure 60

【図６１】

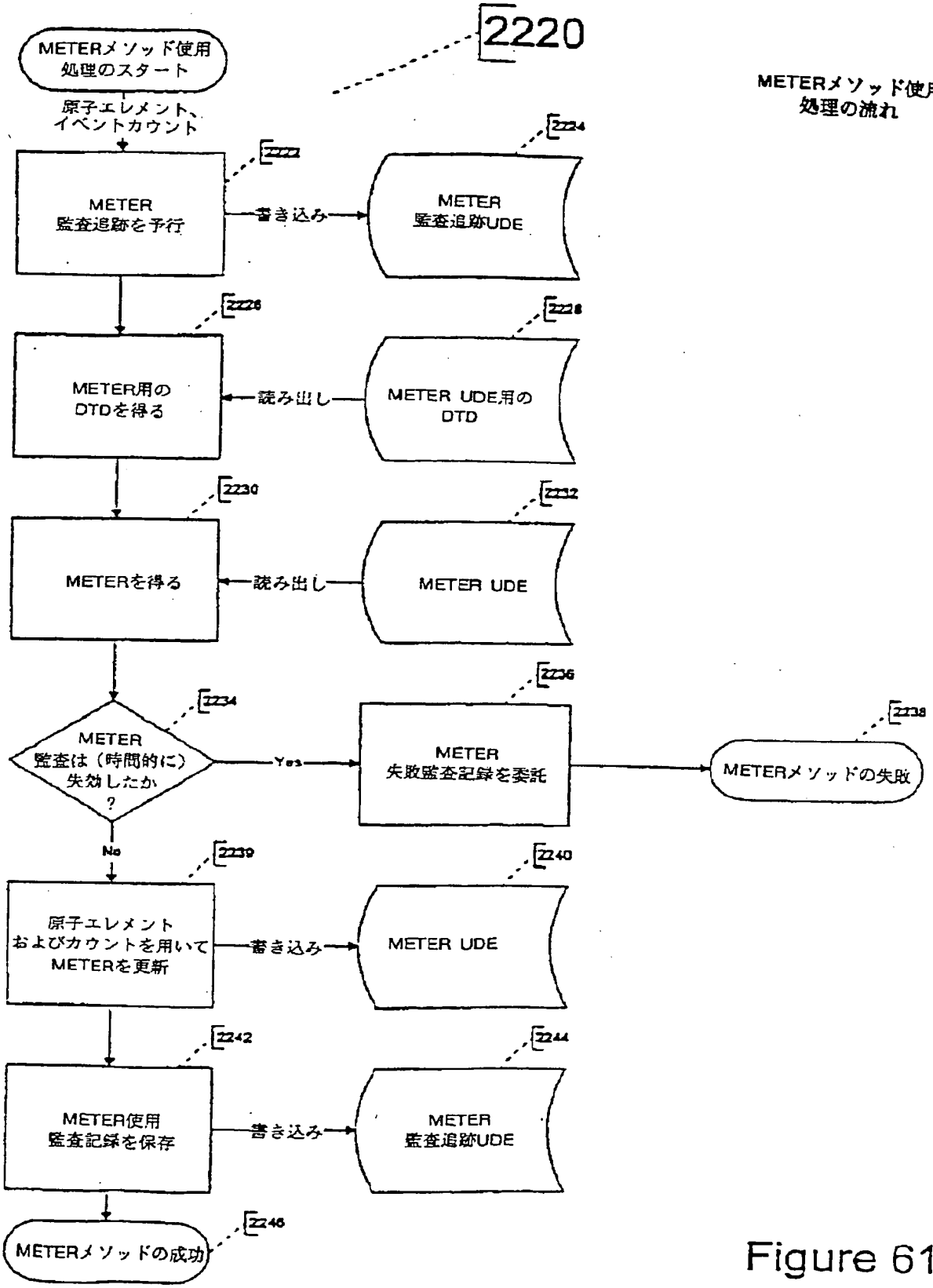
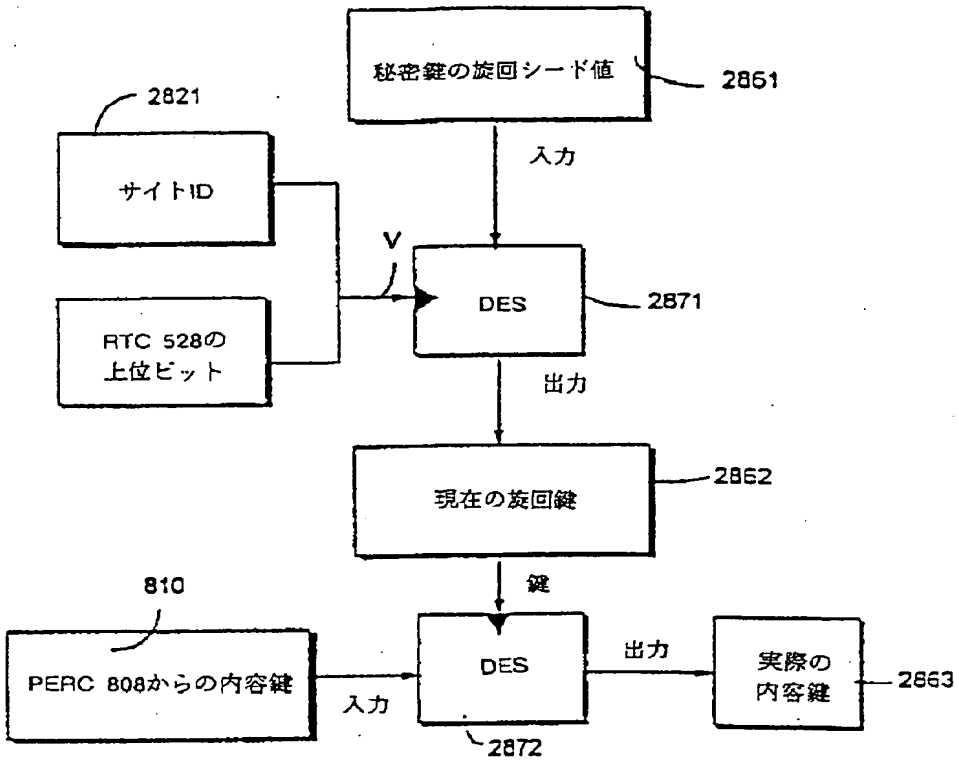


Figure 61

【図６２】

FIG. 62

鍵旋回処理



【図６３】

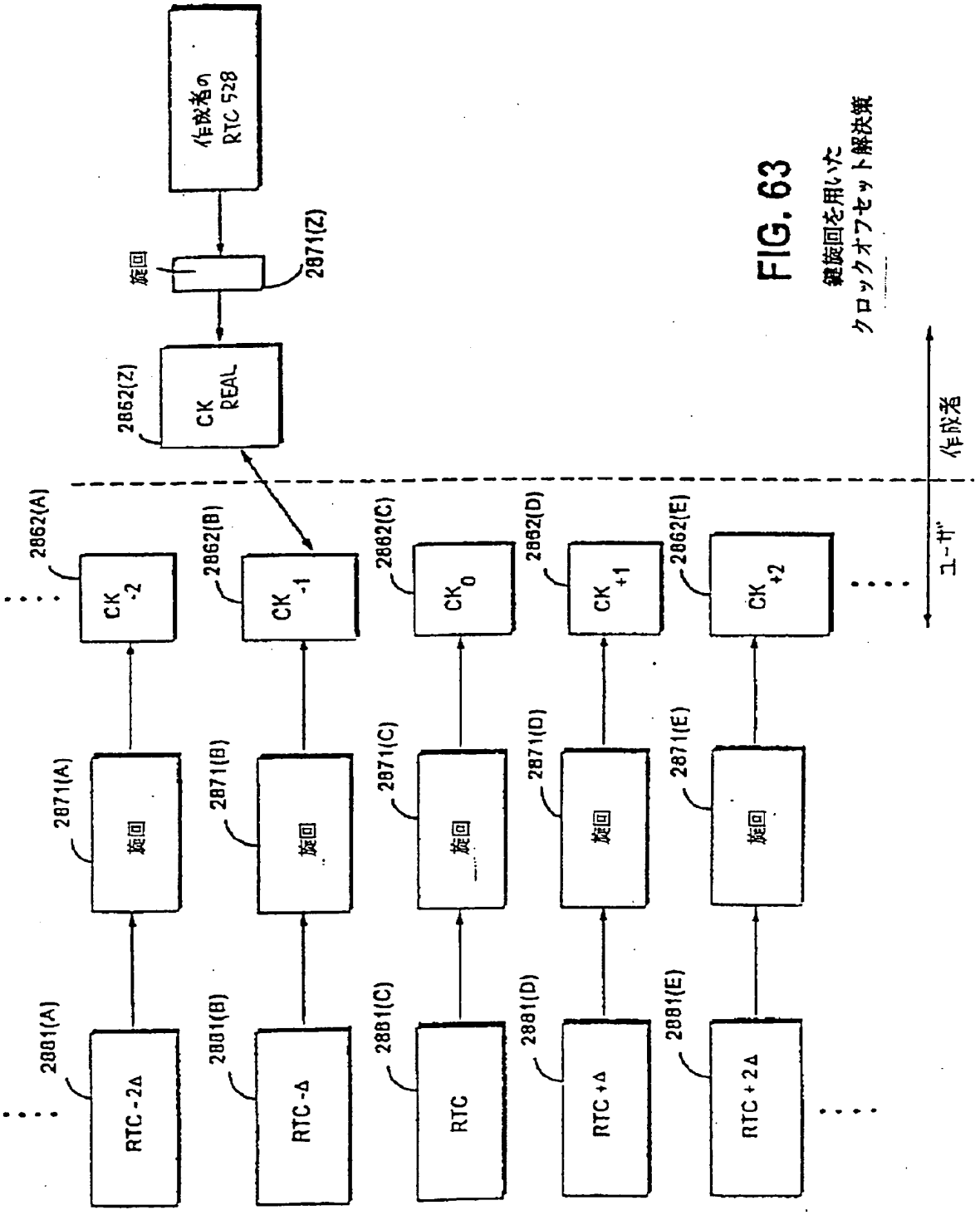
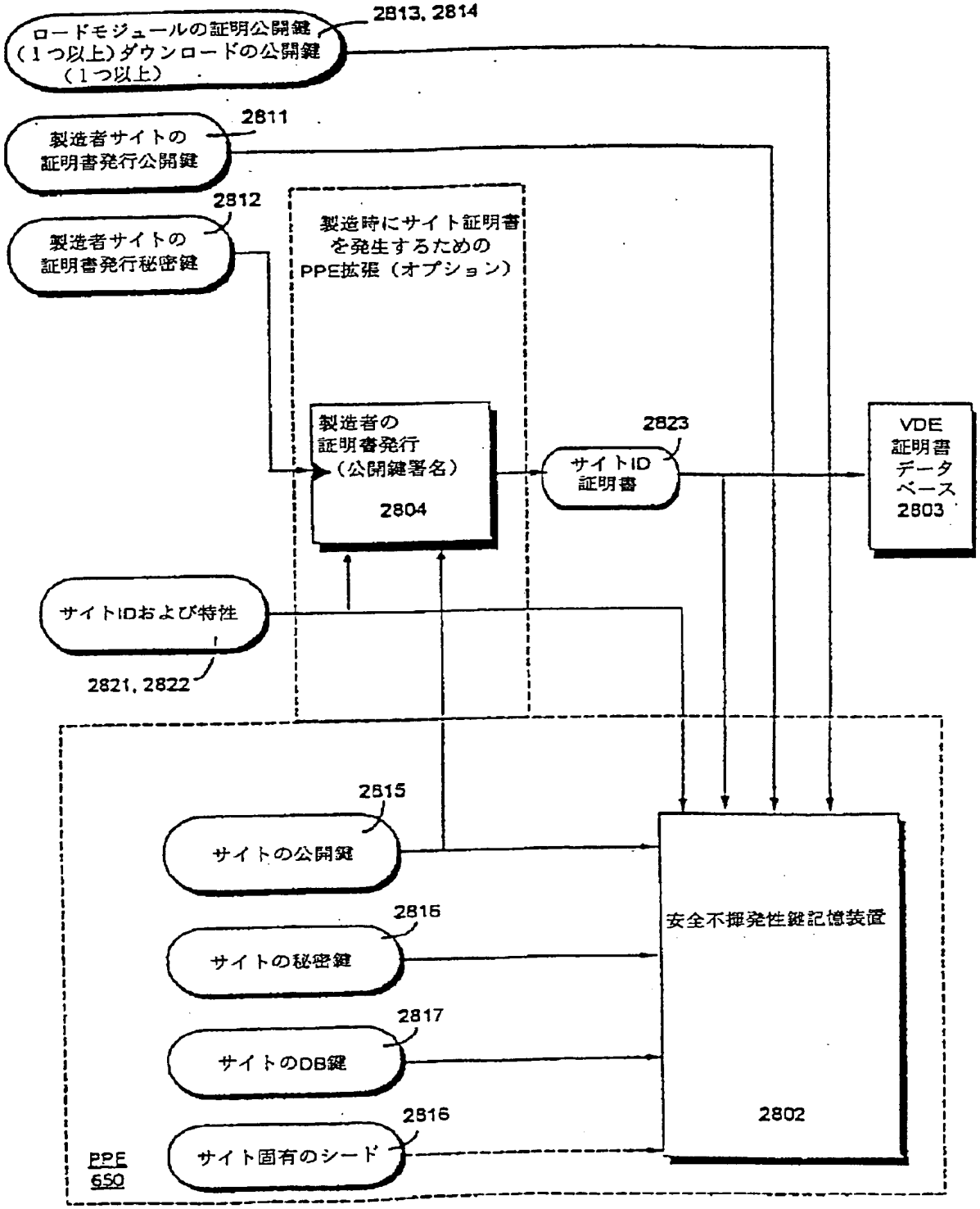


FIG. 63
鍵旋回を用いた
クロックオフセット解決策

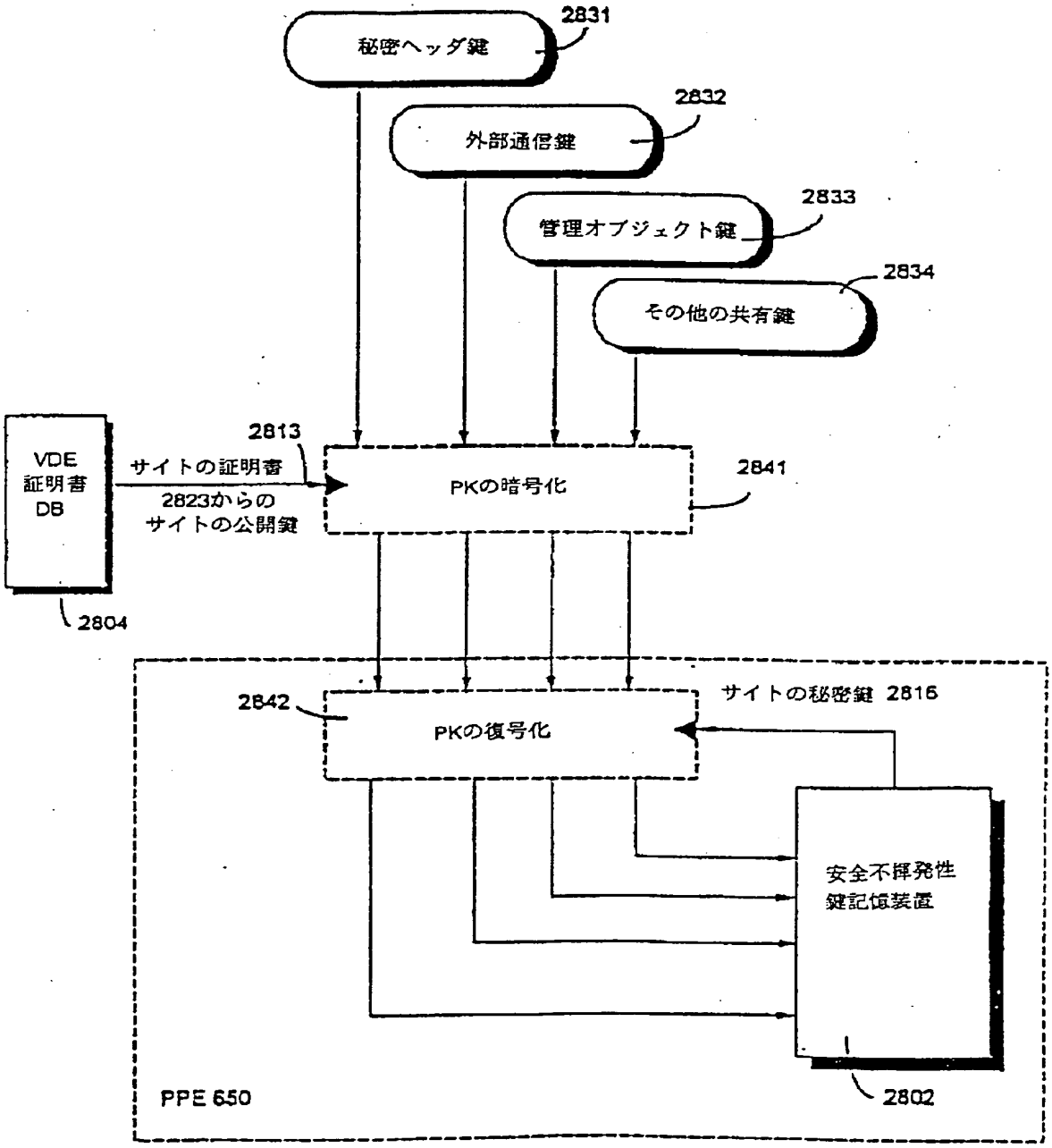
【図６４】

FIG. 64 SPUの鍵初期化／インストレーション



【図６５】

FIG. 65　鍵のインストレーションと更新



【図６６】

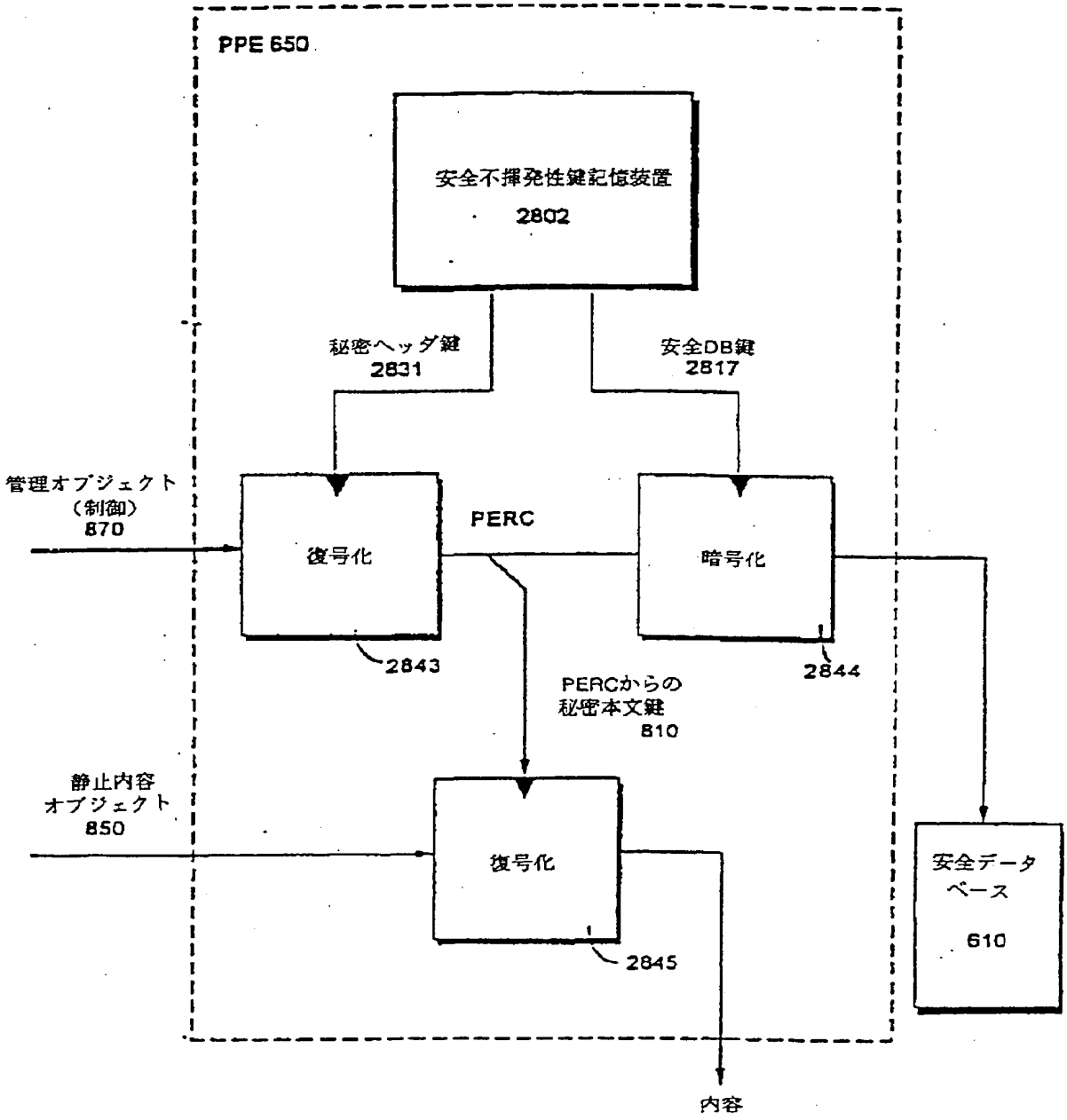


FIG. 66　静止オブジェクトの復号化

【図６７】

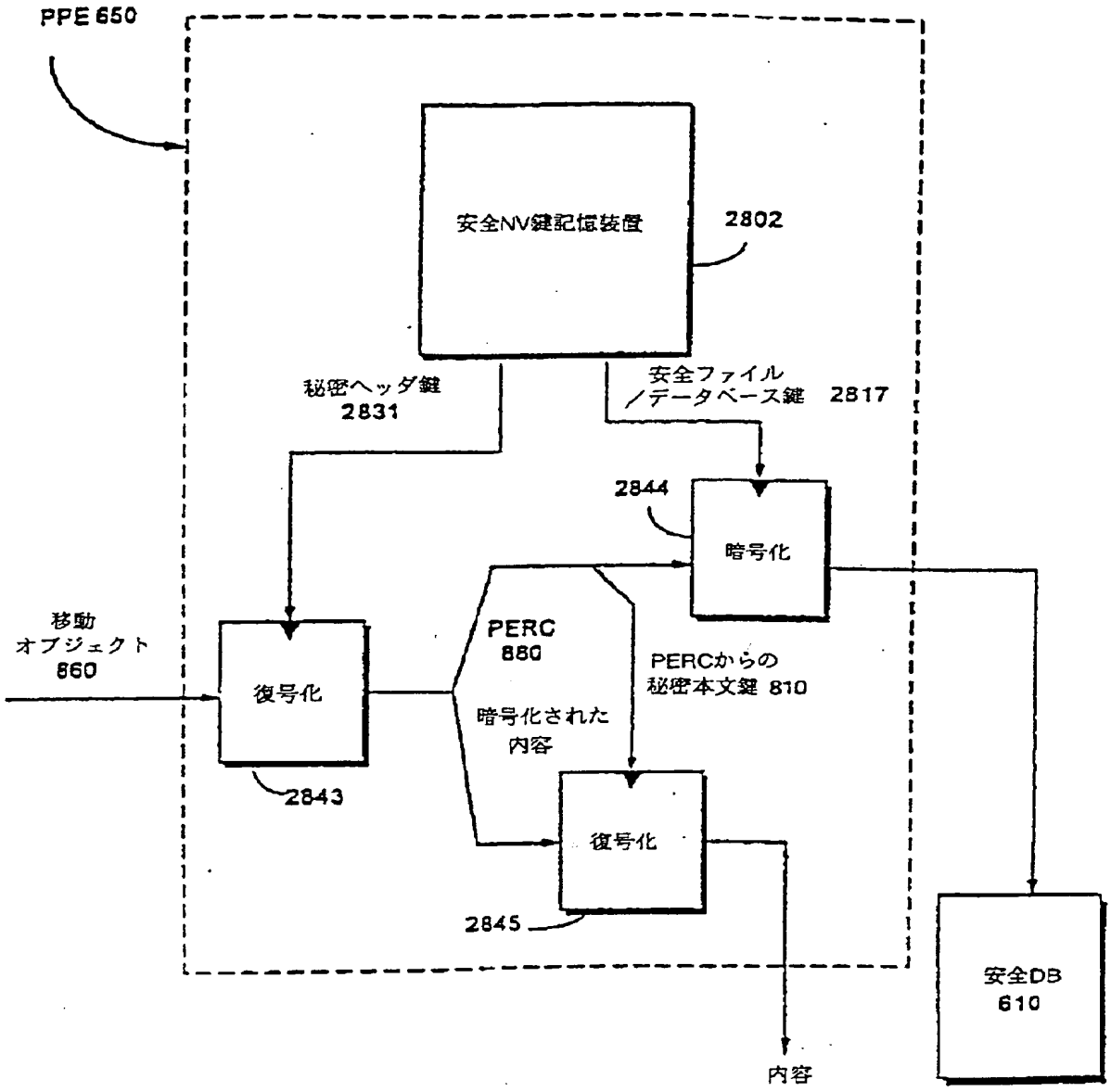


FIG. 67　移動オブジェクトの復号化

【図６８】

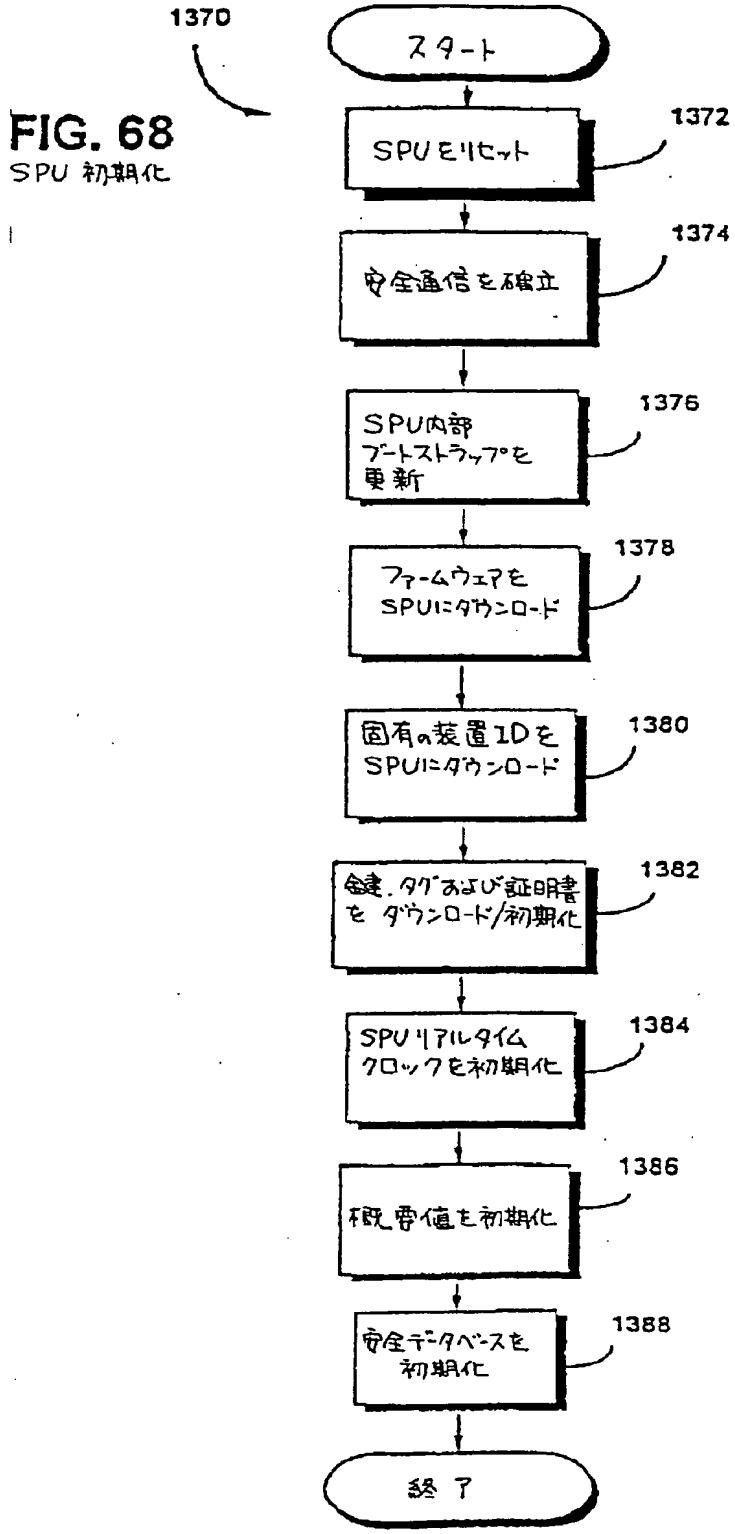


FIG. 68
SPU 初期化

【図６９】

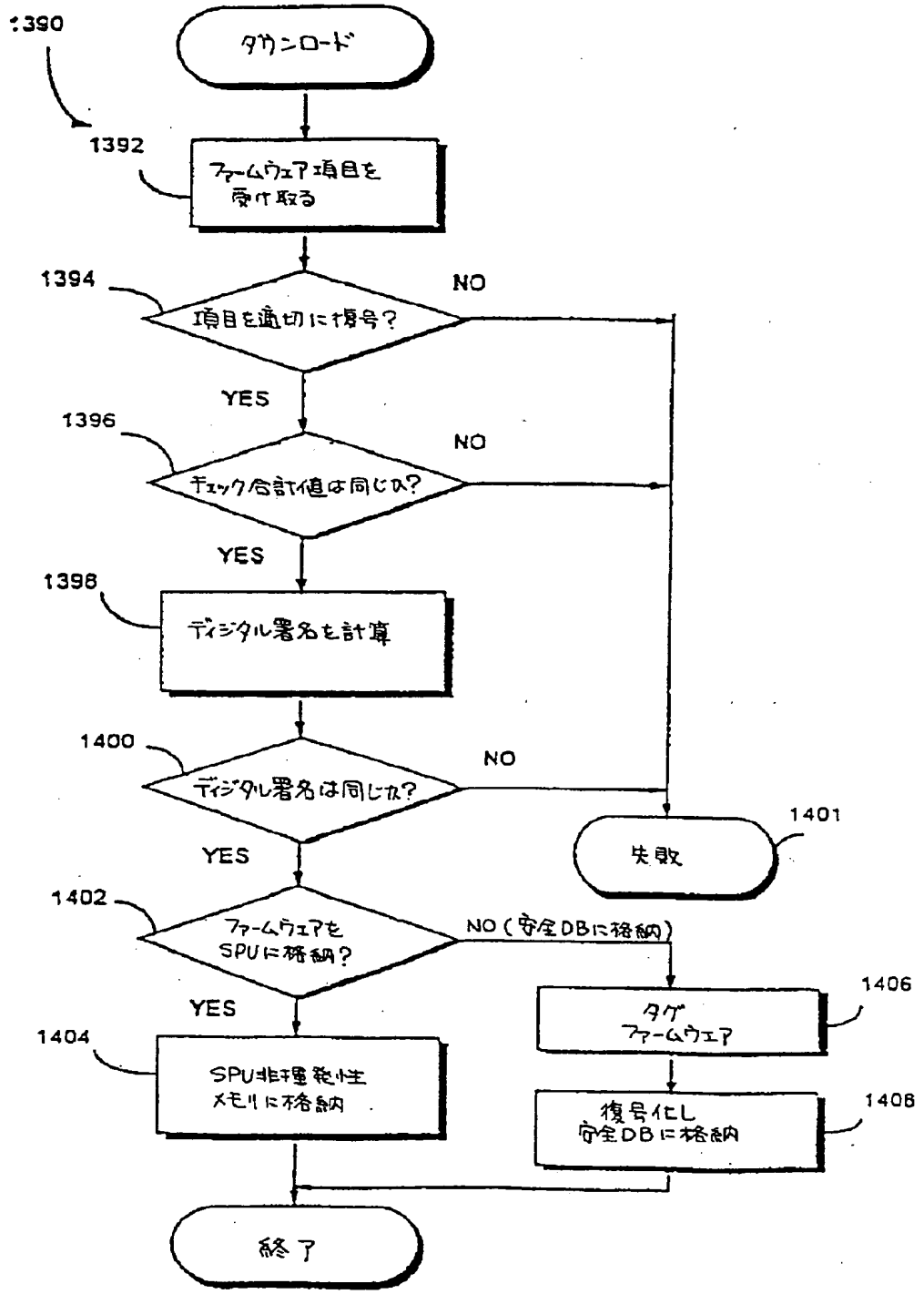


FIG. 69

SPU ファームウェア
ダウンロード

【図７０】

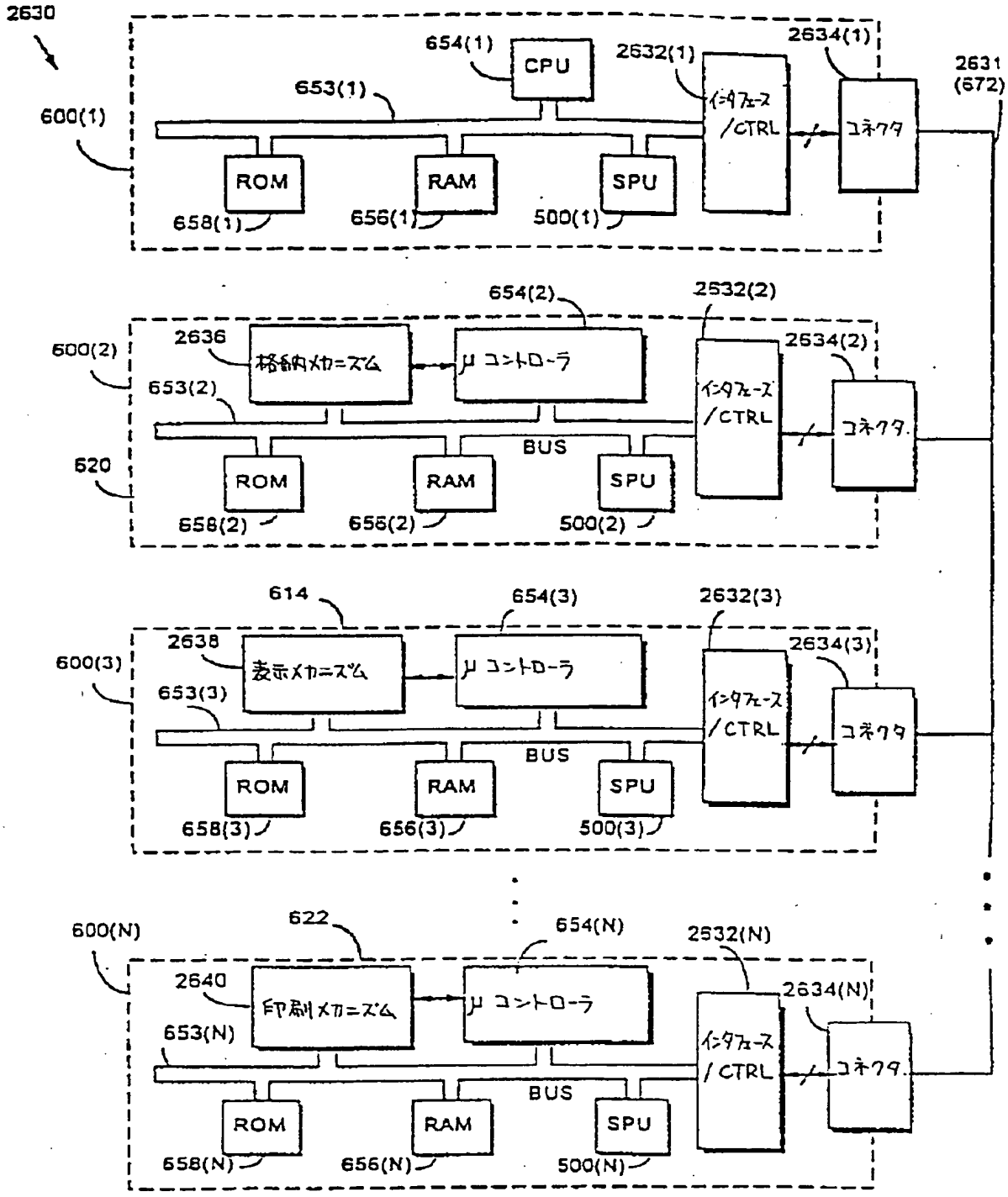
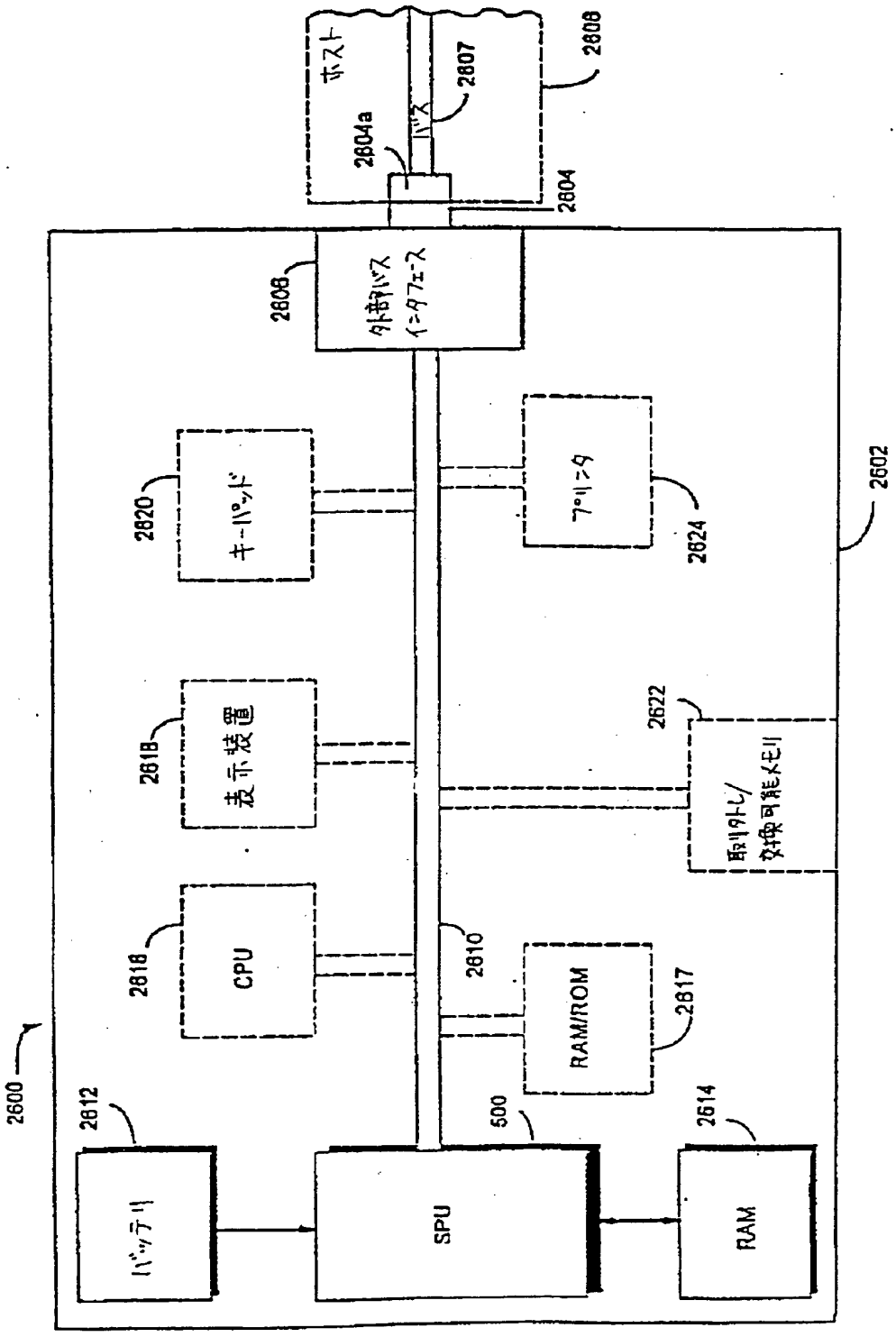

2630
600(1)
654(1)
CPU
653(1)
2632(1)
インタフェース/CTRL
2634(1)
コネクタ
2631
(672)
ROM
RAM
SPU
658(1)
656(1)
500(1)
654(2)
2632(2)
600(2)
2636
格納メカニズム
μコントローラ
2634(2)
653(2)
BUS
620
658(2)
656(2)
500(2)
614
654(3)
2632(3)
600(3)
2638
表示メカニズム
2634(3)
653(3)
658(3)
656(3)
500(3)
600(N)
622
654(N)
2632(N)
2640
印刷メカニズム
2634(N)
653(N)
658(N)
656(N)
500(N)

FIG. 70

【図７１】

FIG. 71
携帯機器



【図７２】

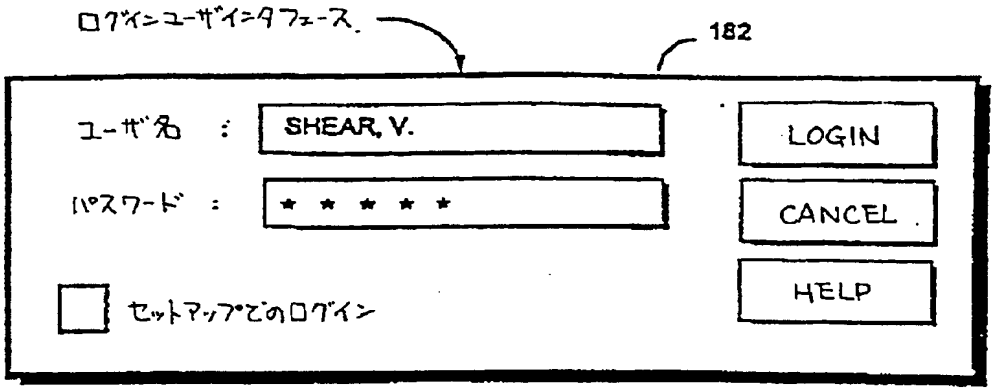
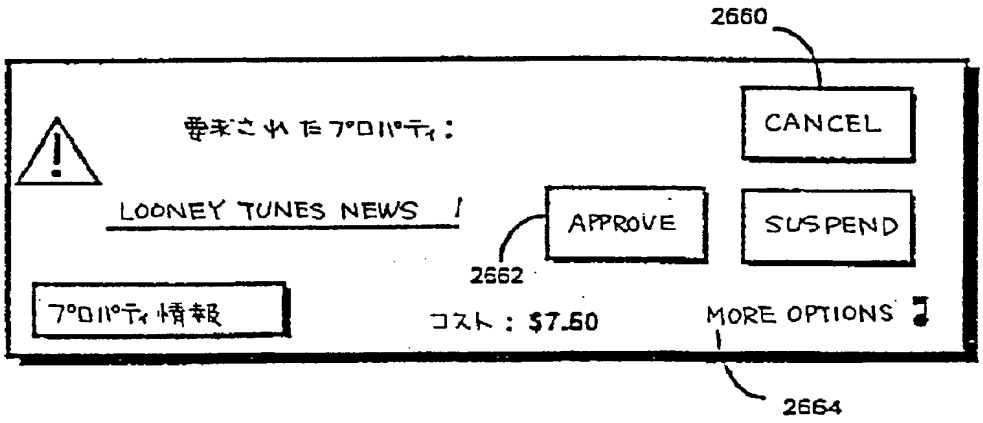


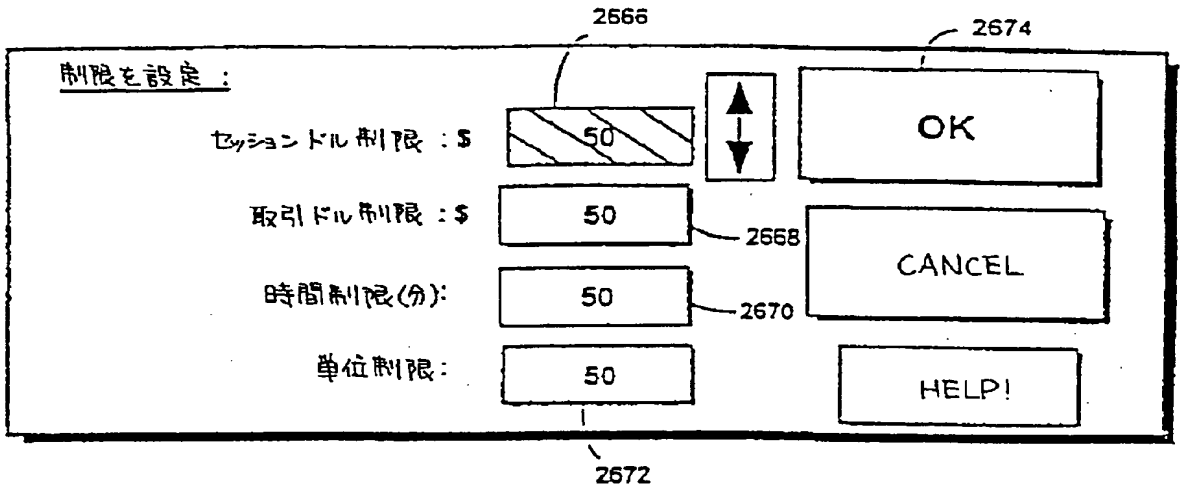
FIG. 72A

FIG. 72B



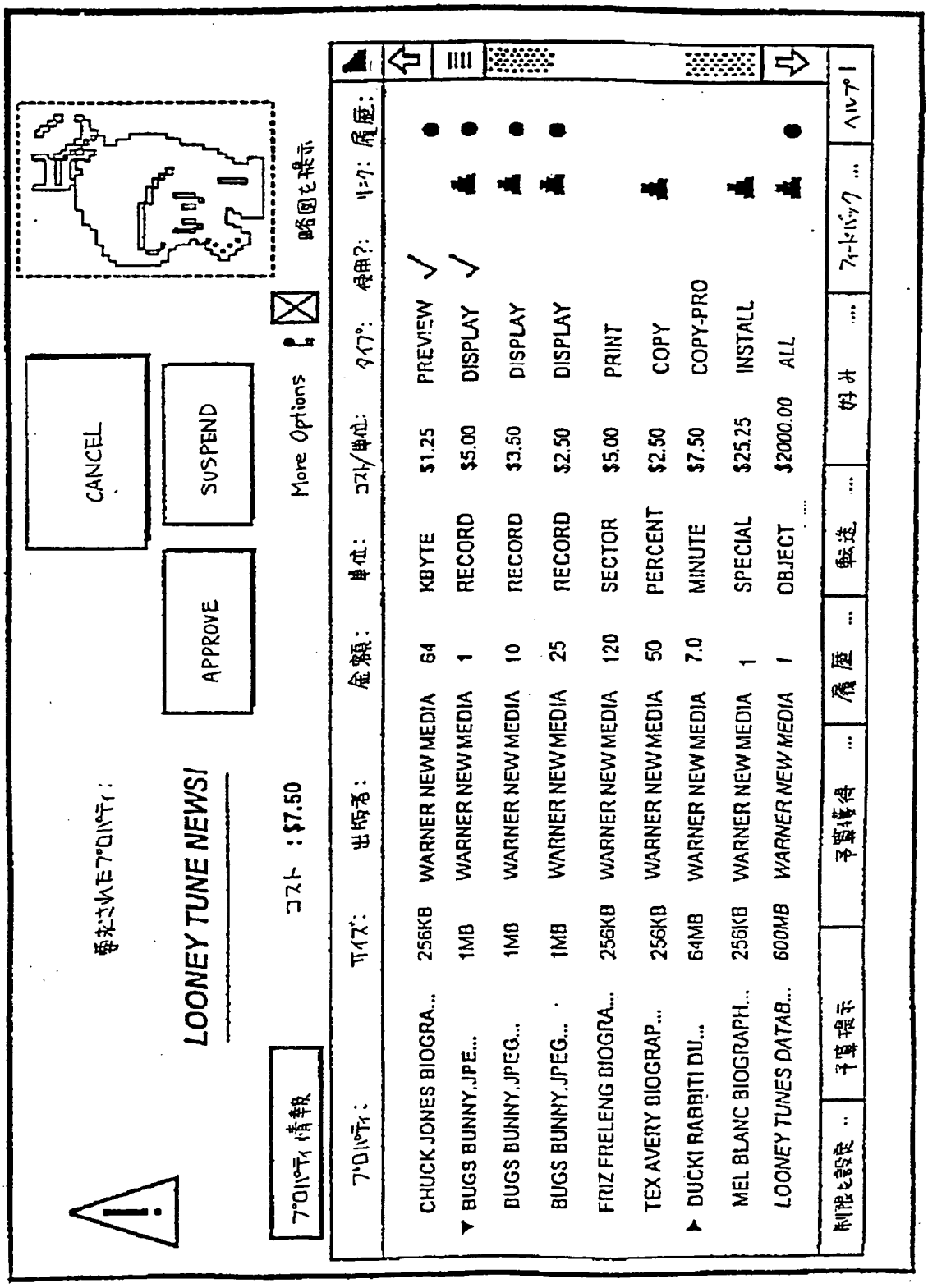
【図７２】

FIG. 72C


2666
2674
制限を設定：
セッションドル制限：$
50
OK
取引ドル制限：$
50
2668
CANCEL
時間制限(分):
50
2670
単位制限:
50
HELP!
2672

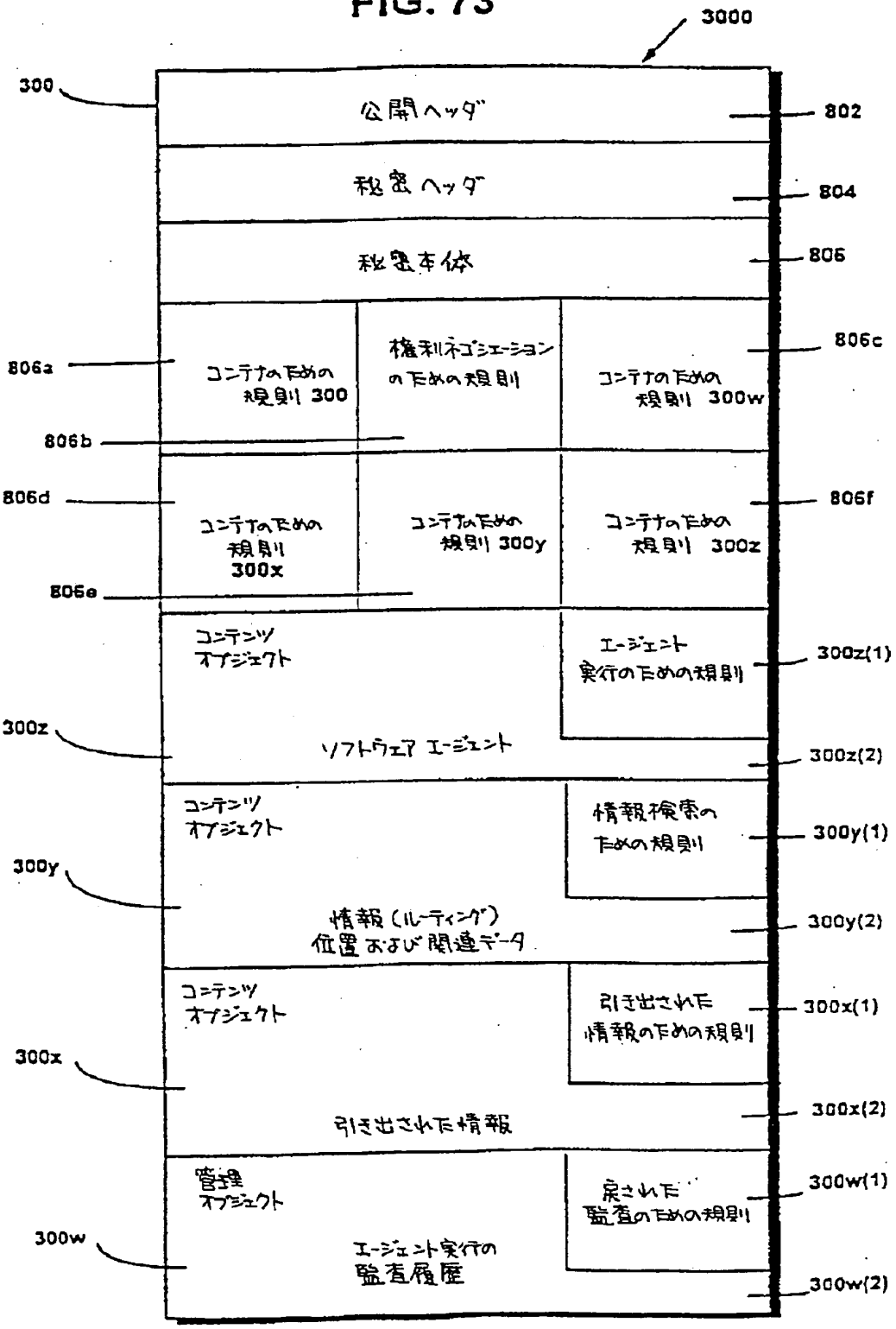
【図72】

FIG. 72D


CANCEL
SUSPEND
APPROVE
More Options
略図を表示
LOONEY TUNE NEWS!
コスト：$7.50
CHUCK JONES BIOGRA... 256KB WARNER NEW MEDIA 64 KBYTE $1.25 PREVIEW
BUGS BUNNY.JPE... 1MB WARNER NEW MEDIA 1 RECORD $5.00 DISPLAY
BUGS BUNNY.JPEG... 1MB WARNER NEW MEDIA 10 RECORD $3.50 DISPLAY
BUGS BUNNY.JPEG... 1MB WARNER NEW MEDIA 25 RECORD $2.50 DISPLAY
FRIZ FRELENG BIOGRA... 256KB WARNER NEW MEDIA 120 SECTOR $5.00 PRINT
TEX AVERY BIOGRAP... 256KB WARNER NEW MEDIA 50 PERCENT $2.50 COPY
DUCKI RABBITI DU... 64MB WARNER NEW MEDIA 7.0 MINUTE $7.50 COPY-PRO
MEL BLANC BIOGRAPH... 256KB WARNER NEW MEDIA 1 SPECIAL $25.25 INSTALL
LOONEY TUNES DATAB... 600MB WARNER NEW MEDIA 1 OBJECT $2000.00 ALL

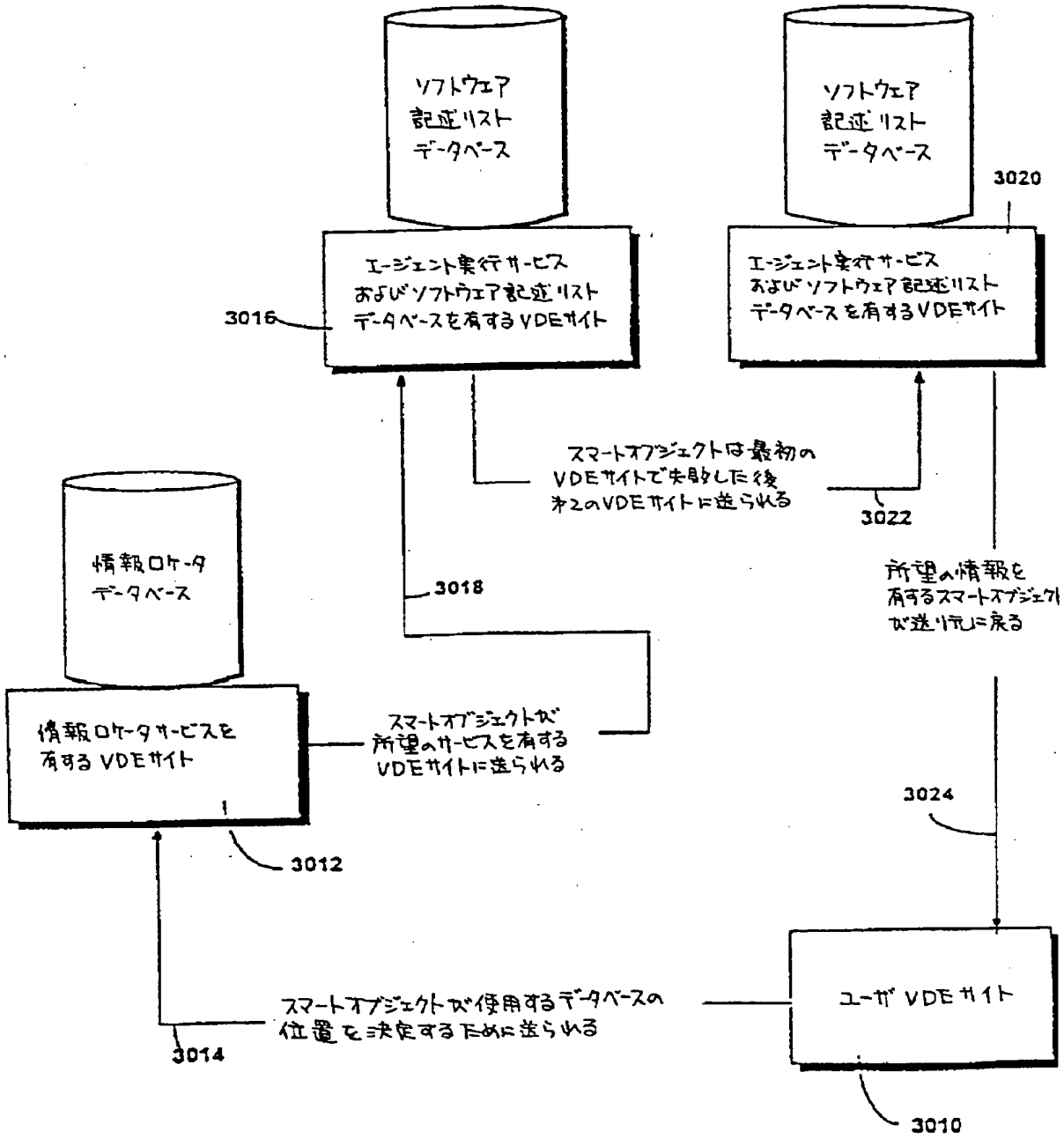
【図７３】

FIG. 73


3000
300
公開ヘッダ
802
秘密ヘッダ
804
秘密本体
806
806a
コンテナのための規則 300
権利ネゴシエーションのための規則
806c
コンテナのための規則 300w
806b
806d
コンテナのための規則 300x
コンテナのための規則 300y
806f
806e
コンテンツオブジェクト
エージェント実行のための規則
300z(1)
300z
ソフトウェア エージェント
300z(2)
コンテンツオブジェクト
情報検索のための規則
300y(1)
300y
情報（ルーティング）位置および関連データ
300y(2)
コンテンツオブジェクト
引き出された情報のための規則
300x(1)
300x
引き出された情報
300x(2)
管理オブジェクト
戻された監査のための規則
300w(1)
300w
エージェント実行の監査履歴
300w(2)

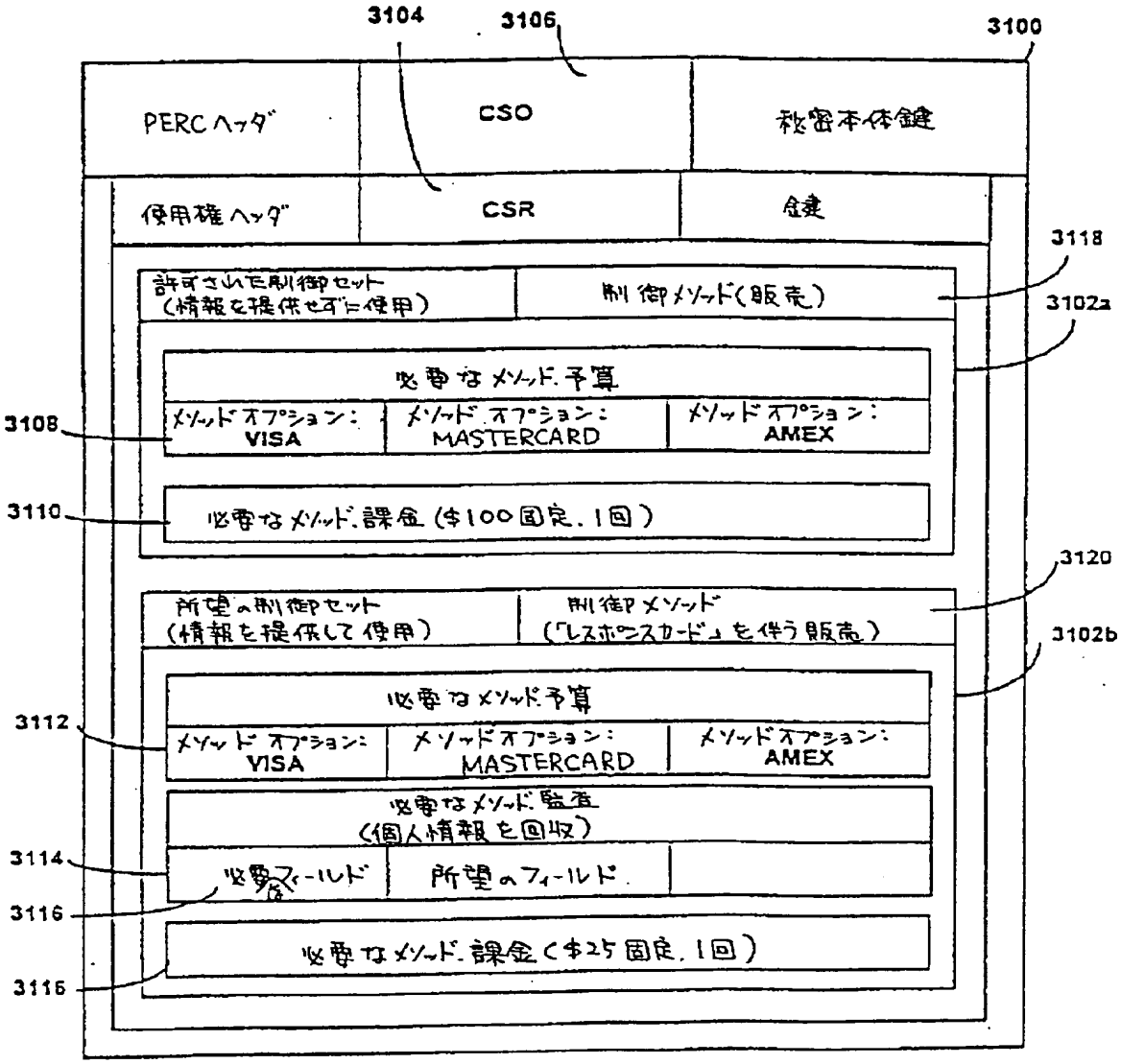
【図７４】

FIG. 74


ソフトウェア
記述リスト
データベース
ソフトウェア
記述リスト
データベース
3020
エージェント実行サービス
およびソフトウェア記述リスト
データベースを有するVDEサイト
3016
エージェント実行サービス
およびソフトウェア記述リスト
データベースを有するVDEサイト
スマートオブジェクトは最初の
VDEサイトで実動した後
次のVDEサイトに送られる
3022
情報ロケータ
データベース
3018
所望の情報を
有するスマートオブジェクト
が送り元に戻る
情報ロケータサービスを
有するVDEサイト
スマートオブジェクトが
所望のサービスを有する
VDEサイトに送られる
3024
3012
スマートオブジェクトが使用するデータベースの
位置を決定するために送られる
ユーザVDEサイト
3014
3010

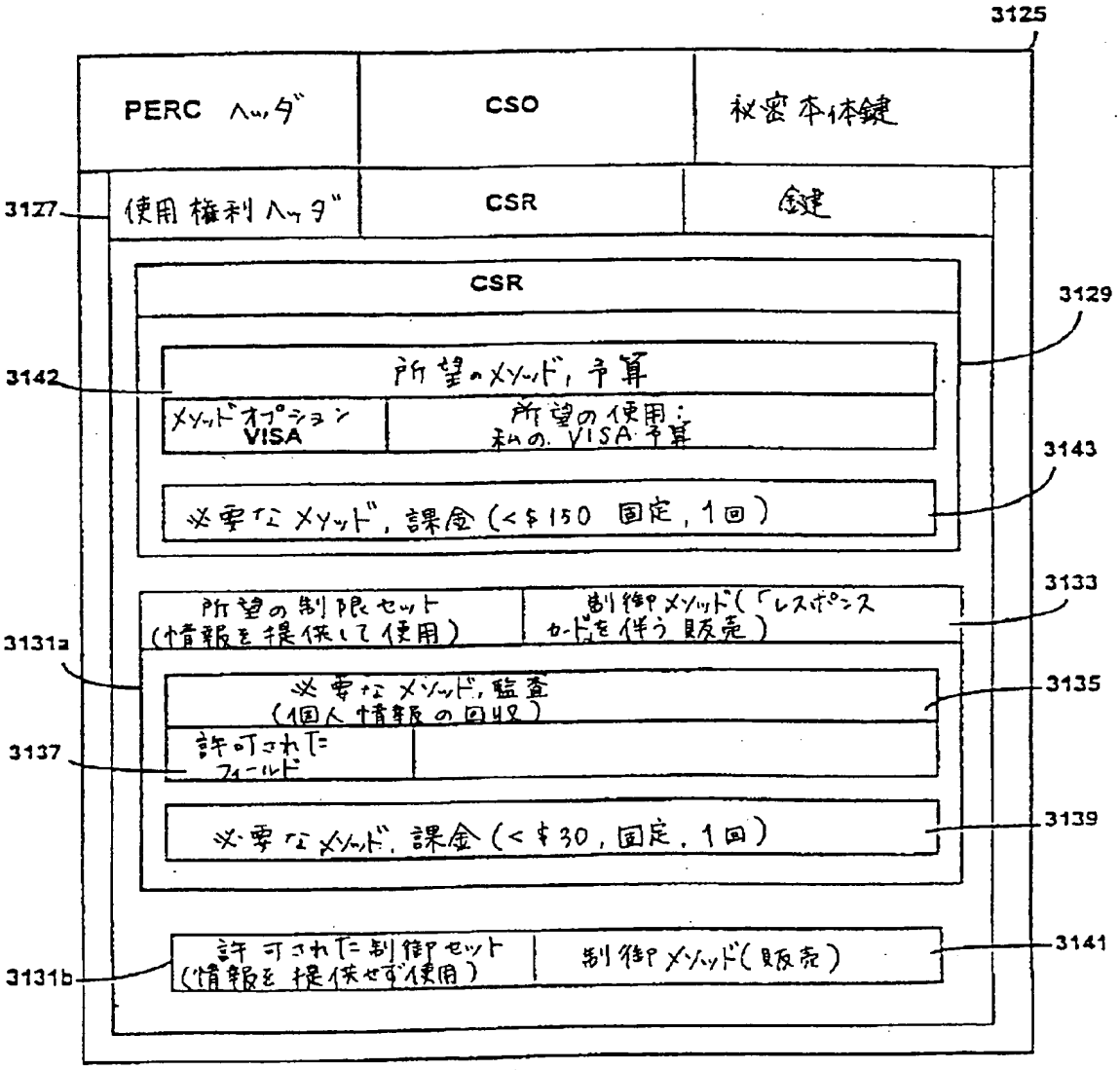
【図７５】

FIG. 75A


3104
3106
3100
PERCヘッダ
CSO
秘密本体鍵
使用権ヘッダ
CSR
鍵
3118
許すされた制御セット
(情報を提供せずに使用)
制御メソッド(販売)
3102a
必要なメソッド予算
3108
メソッドオプション:
VISA
メソッドオプション:
MASTERCARD
メソッドオプション:
AMEX
3110
必要なメソッド課金($100固定、1回)
3120
所望の制御セット
(情報を提供して使用)
制御メソッド
(「レスポンスカード」を伴う販売)
3102b
必要なメソッド予算
3112
メソッドオプション:
VISA
メソッドオプション:
MASTERCARD
メソッドオプション:
AMEX
必要なメソッド監査
(個人情報を回収)
3114
必要なフィールド
所望のフィールド
3116
必要なメソッド課金($25固定、1回)
3115

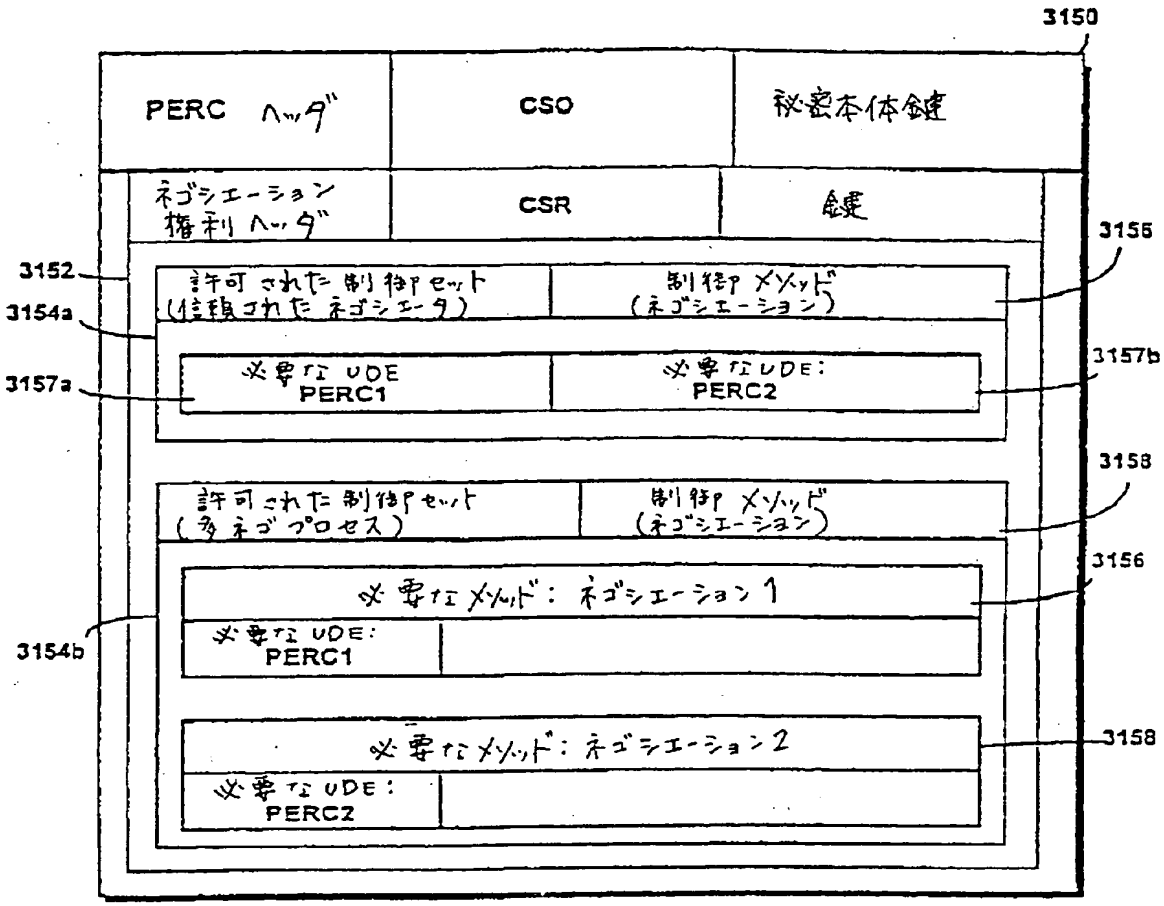
【図７５】

FIG. 75B


3125
PERC ヘッダ
CSO
秘密本体鍵
3127
使用権利ヘッダ
CSR
鍵
CSR
3129
所望のメソッド，予算
3142
メソッドオプション VISA
所望の使用：私の VISA 予算
3143
必要なメソッド，課金（<$150 固定，1回）
所望の制限セット（情報を提供して使用）
制御メソッド（「レスポンスカードを伴う販売）
3133
3131a
必要なメソッド，監査（個人情報の回収）
3135
3137
許可されたフィールド
必要なメソッド，課金（<$30，固定，1回）
3139
許可された制御セット（情報を提供せず使用）
制御メソッド（販売）
3141
3131b

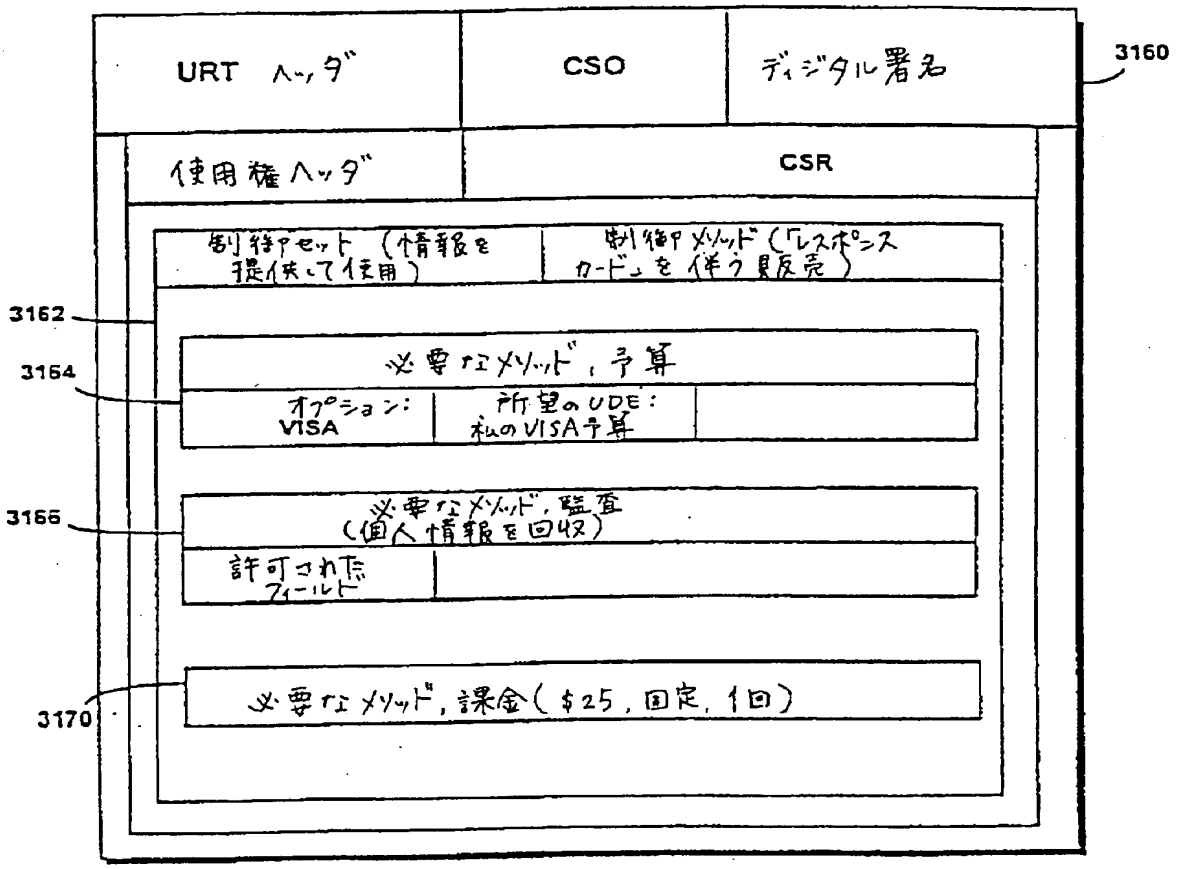
［図７５］

FIG. 75C


3150
PERC ヘッダ
CSO
秘密本体鍵
ネゴシエーション 権利 ヘッダ
CSR
鍵
3155
3152
許可された制御セット (信頼されたネゴシエータ)
制御メソッド (ネゴシエーション)
3154a
3157b
3157a
必要なUDE PERC1
必要なUDE: PERC2
3158
許可された制御セット (多ネゴプロセス)
制御メソッド (ネゴシエーション)
3156
必要なメソッド: ネゴシエーション1
3154b
必要なUDE: PERC1
必要なメソッド: ネゴシエーション2
3158
必要なUDE: PERC2

【図７５】

FIG. 75D


URT ヘッダ
CSO
ディジタル署名
3160
使用権ヘッダ
CSR
制御アセット（情報を提供して使用）
制御メソッド（「レスポンスカード」を伴う見返完）
3162
必要なメソッド，予算
3164
オプション：VISA
所望のUDE：私のVISA予算
必要なメソッド，監査（個人情報を回収）
3166
許可されたフィールド
必要なメソッド，課金（$25，固定，1回）
3170

［図７５］

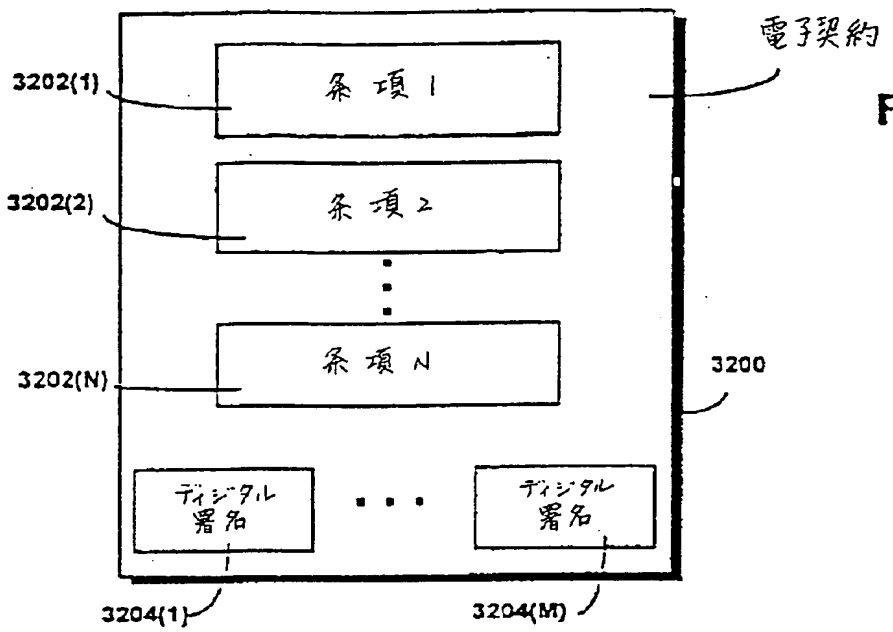


FIG. 75E

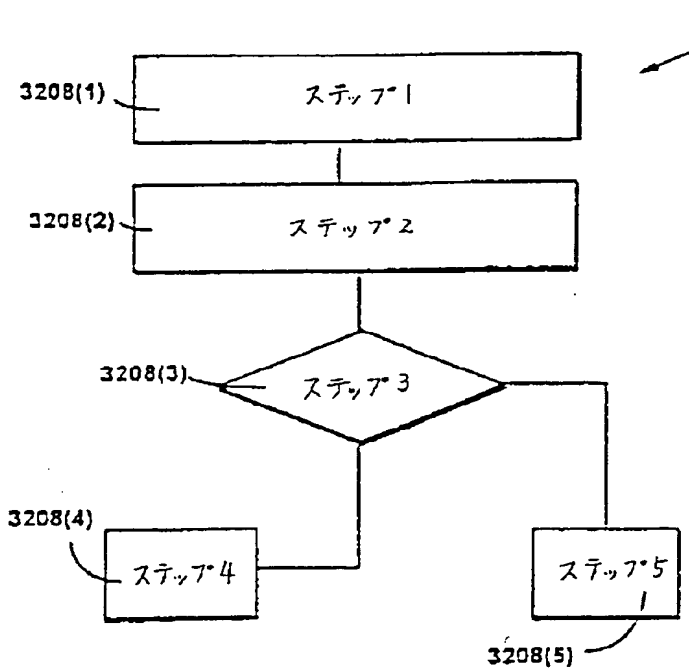
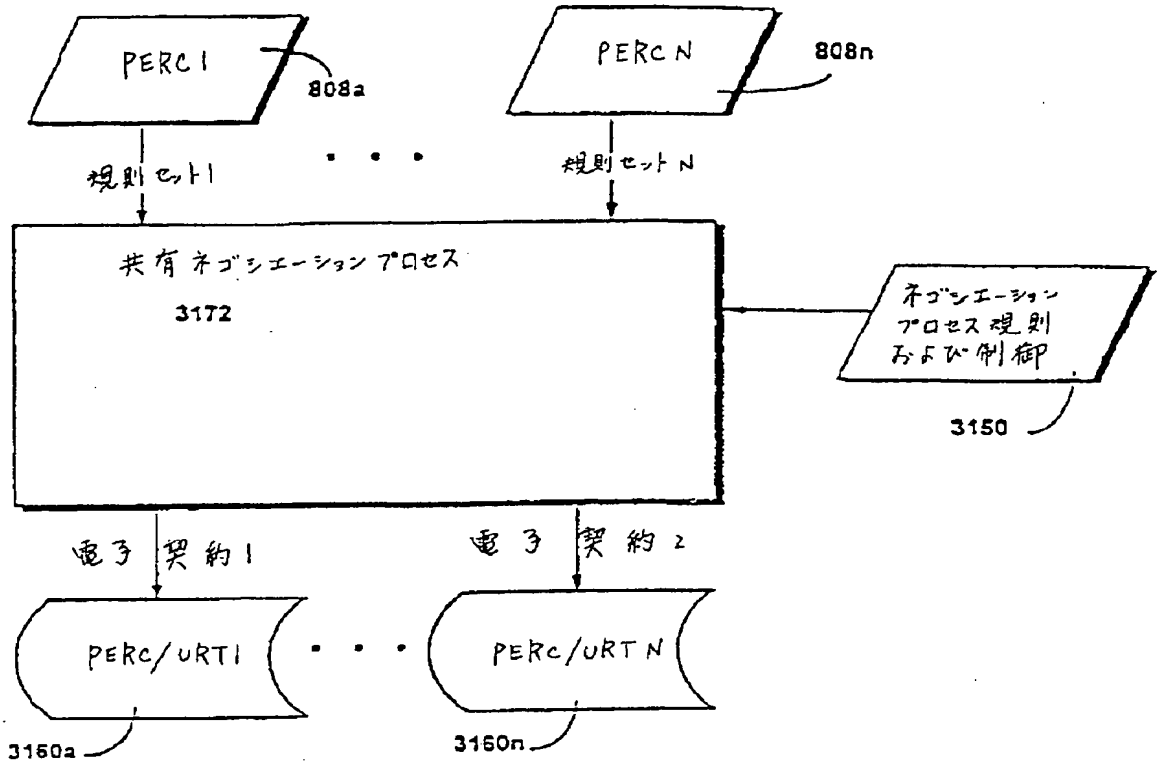


FIG. 75F

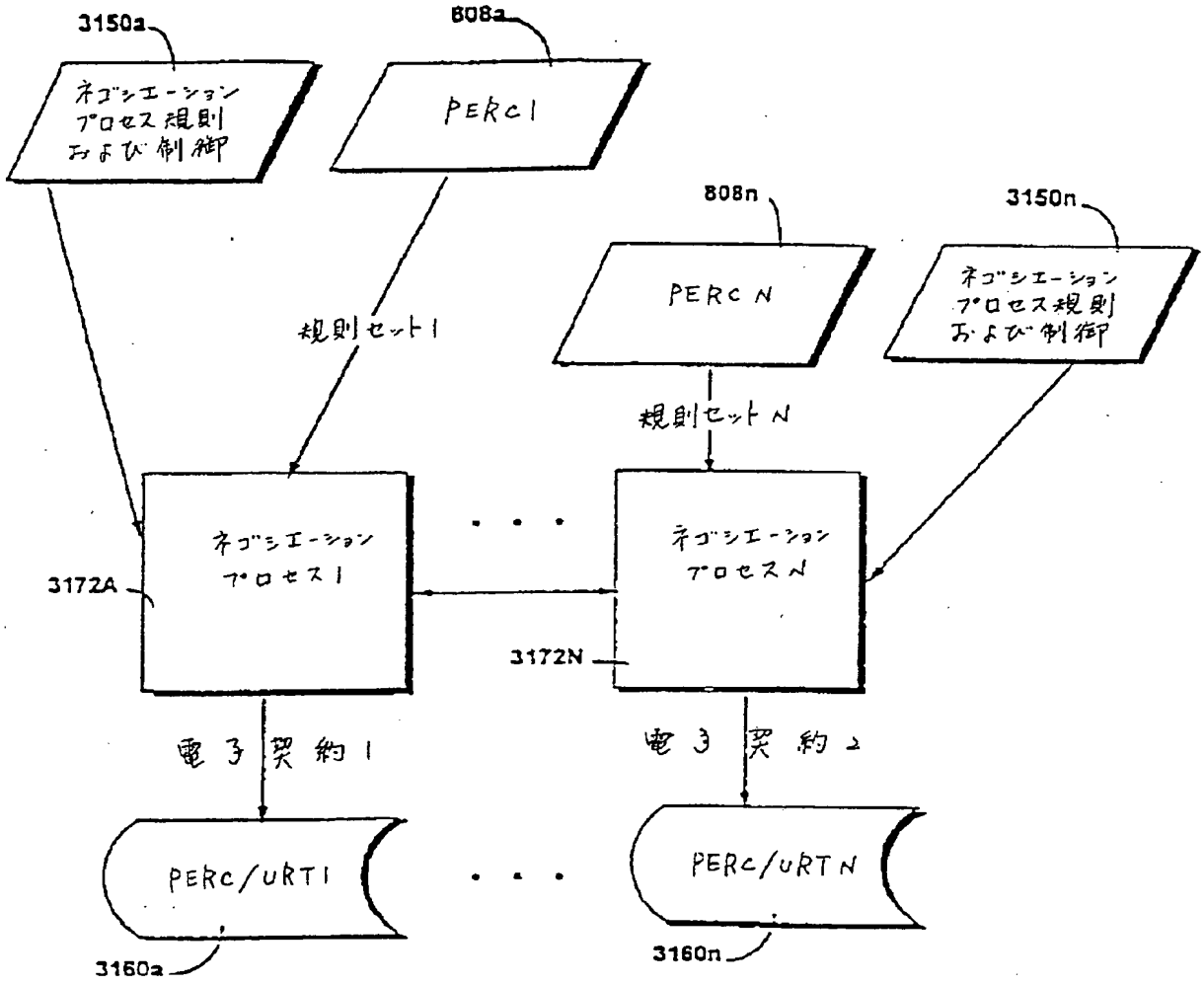
【図７６】

FIG. 76A


PERC 1
808a
PERC N
808n
規則セット1
規則セットN
共有ネゴシエーションプロセス
3172
ネゴシエーション
プロセス規則
および制御
3150
電子契約1
電子契約2
PERC/URT1
PERC/URT N
3160a
3160n

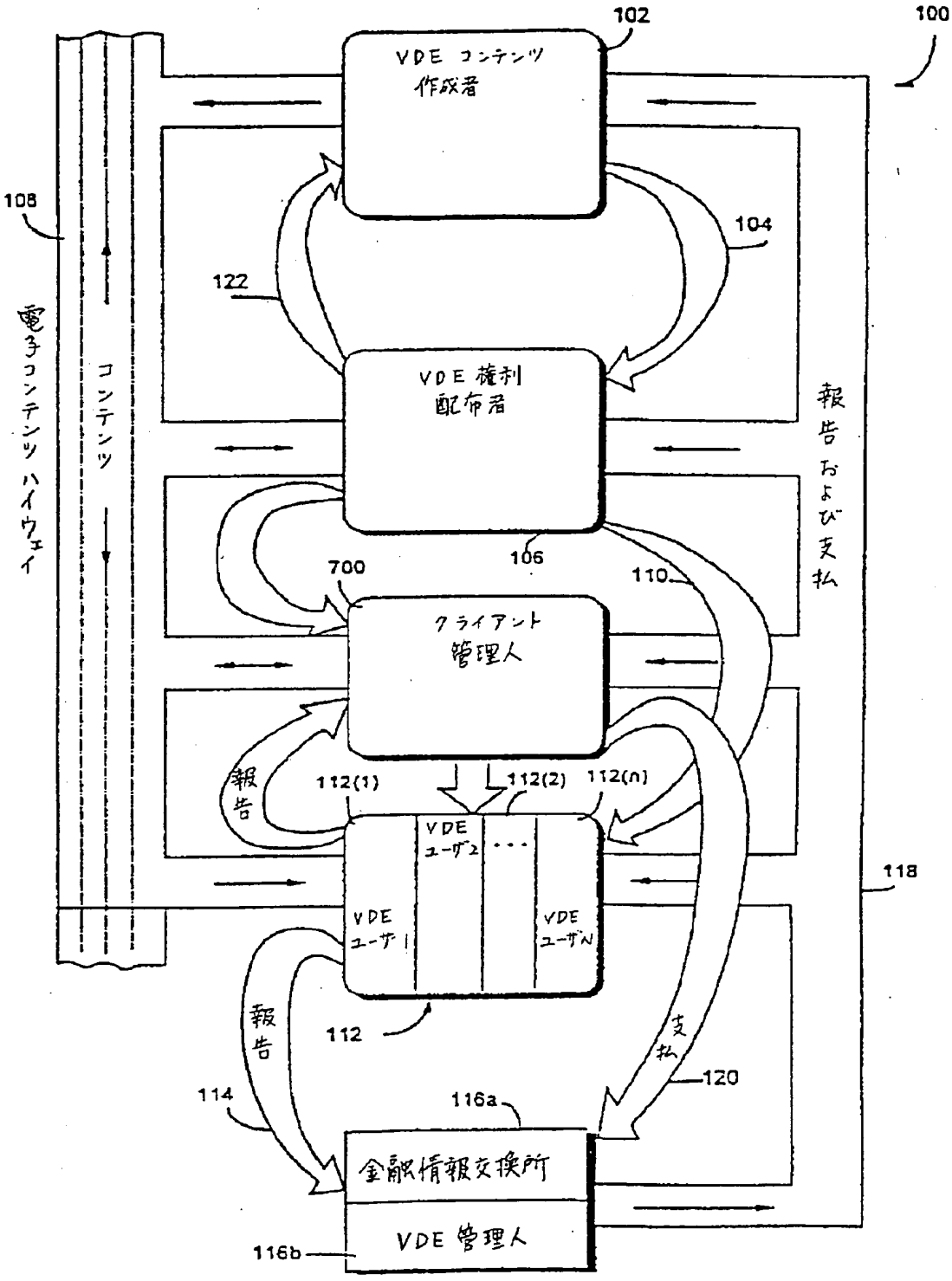
【図７６】

FIG. 76B


3150a
808a
ネゴシエーション
プロセス規則
および制御
PERC1
808n
3150n
PERC N
ネゴシエーション
プロセス規則
および制御
規則セット1
規則セットN
ネゴシエーション
プロセス1
ネゴシエーション
プロセスN
3172A
3172N
電子契約1
電子契約2
PERC/URT1
PERC/URT N
3160a
3160n

【図７７】

FIG. 77


102
100
VDE コンテンツ
作成者
108
104
122
電子コンテンツ ハイウェイ
コンテンツ
VDE 権利
配布者
報告および支払
700
106
110
クライアント
管理人
報告
112(1)
112(2)
112(n)
VDE
ユーザ2
VDE
ユーザ1
VDE
ユーザN
118
報告
112
支払
120
114
116a
金融情報交換所
VDE 管理人
116b

【図７８】

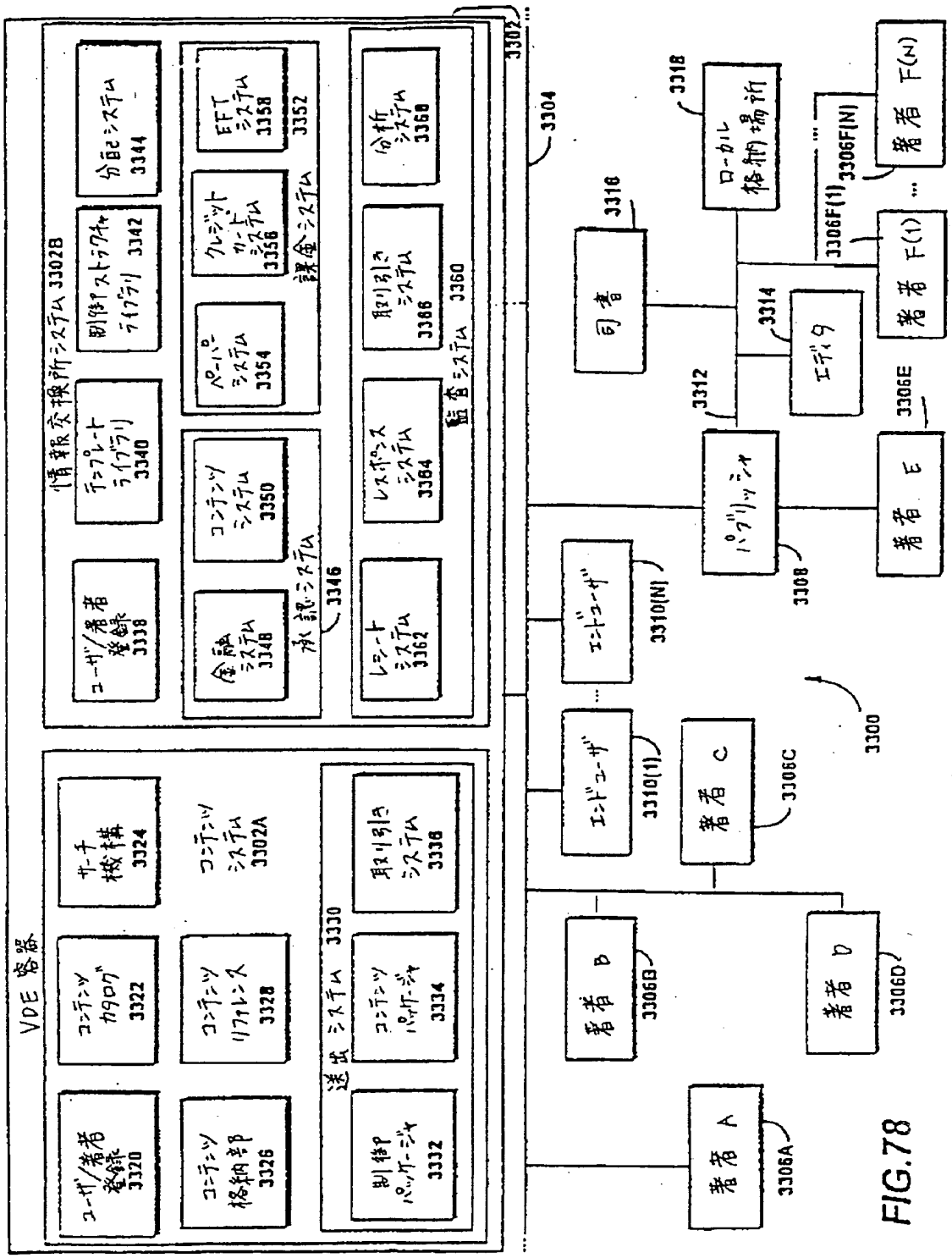
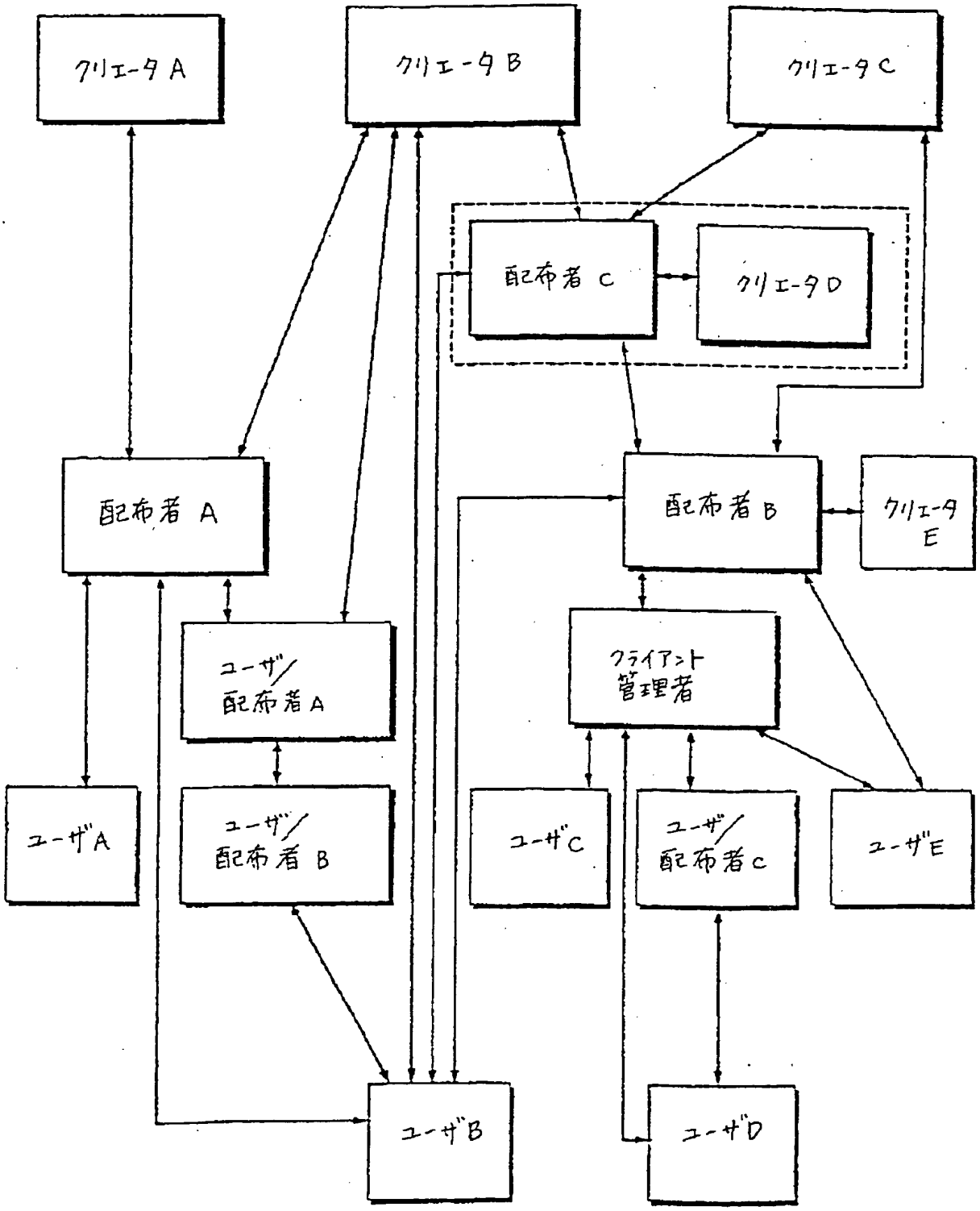

VDE 容器
ユーザ/著者 登録 3320
コンテンツ カタログ 3322
サーチ 機構 3324
コンテンツ 格納部 3326
コンテンツ リファレンス 3328
コンテンツ システム 3302A
則御 パッケージャ 3332
コンテンツ パッケージャ 3334
取引き システム 3336
迷惑 システム 3330
情報交換所システム 3302B
ユーザ/著者 登録 3338
テンプレート ライブラリ 3340
則御ストラクチャ ライブラリ 3342
分配システム 3344
金融 システム 3348
コンテンツ システム 3350
承認システム 3346
レポート システム 3362
レスポンス システム 3364
監査システム 3360
ペーパー システム 3354
クレジット カード システム 3356
EFT システム 3358
課金システム 3352
取引き システム 3366
分析 システム 3368
3302
3304
3316
3318
3312
3314
3306E
3306F(1)
3306F(N)
3310(1)
3310(N)
3308
3300
3306A
3306B
3306C
3306D
著者 A
著者 B
著者 C
著者 D
著者 E
著者 F(1)
著者 F(N)
司書
ローカル 格納場所
エディタ
エンドユーザ
エンドユーザ
パブリッシャ

FIG.78

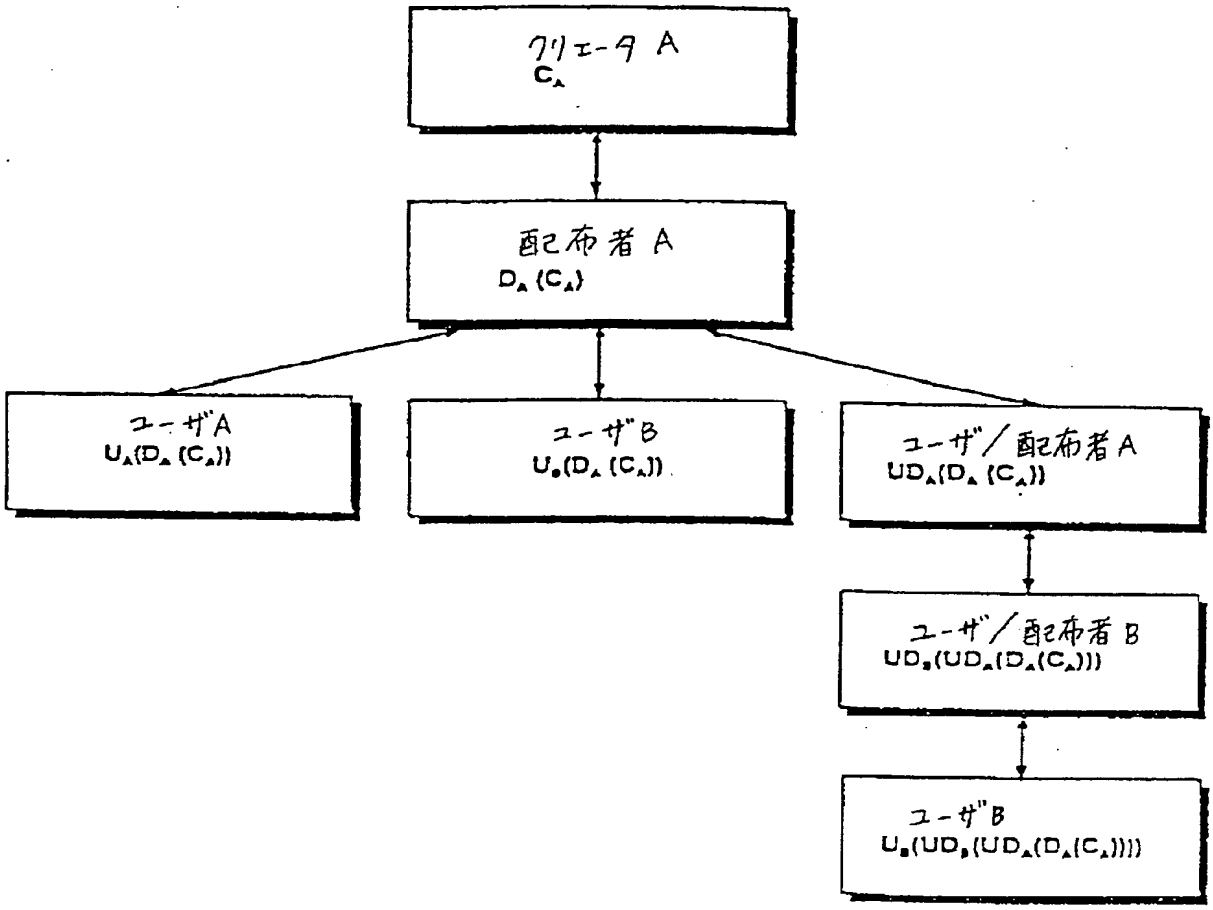
【図７９】

FIG. 79


クリエータA
クリエータB
クリエータC
配布者C
クリエータD
配布者A
配布者B
クリエータE
ユーザ/配布者A
クライアント管理者
ユーザA
ユーザ/配布者B
ユーザC
ユーザ/配布者C
ユーザE
ユーザB
ユーザD

【図80】

FIG. 80


クリエータ A
C_A
配布者 A
$D_A(C_A)$
ユーザA
$U_A(D_A(C_A))$
ユーザB
$U_B(D_A(C_A))$
ユーザ／配布者A
$UD_A(D_A(C_A))$
ユーザ／配布者B
$UD_B(UD_A(D_A(C_A)))$
ユーザB
$U_B(UD_B(UD_A(D_A(C_A))))$

【図81】

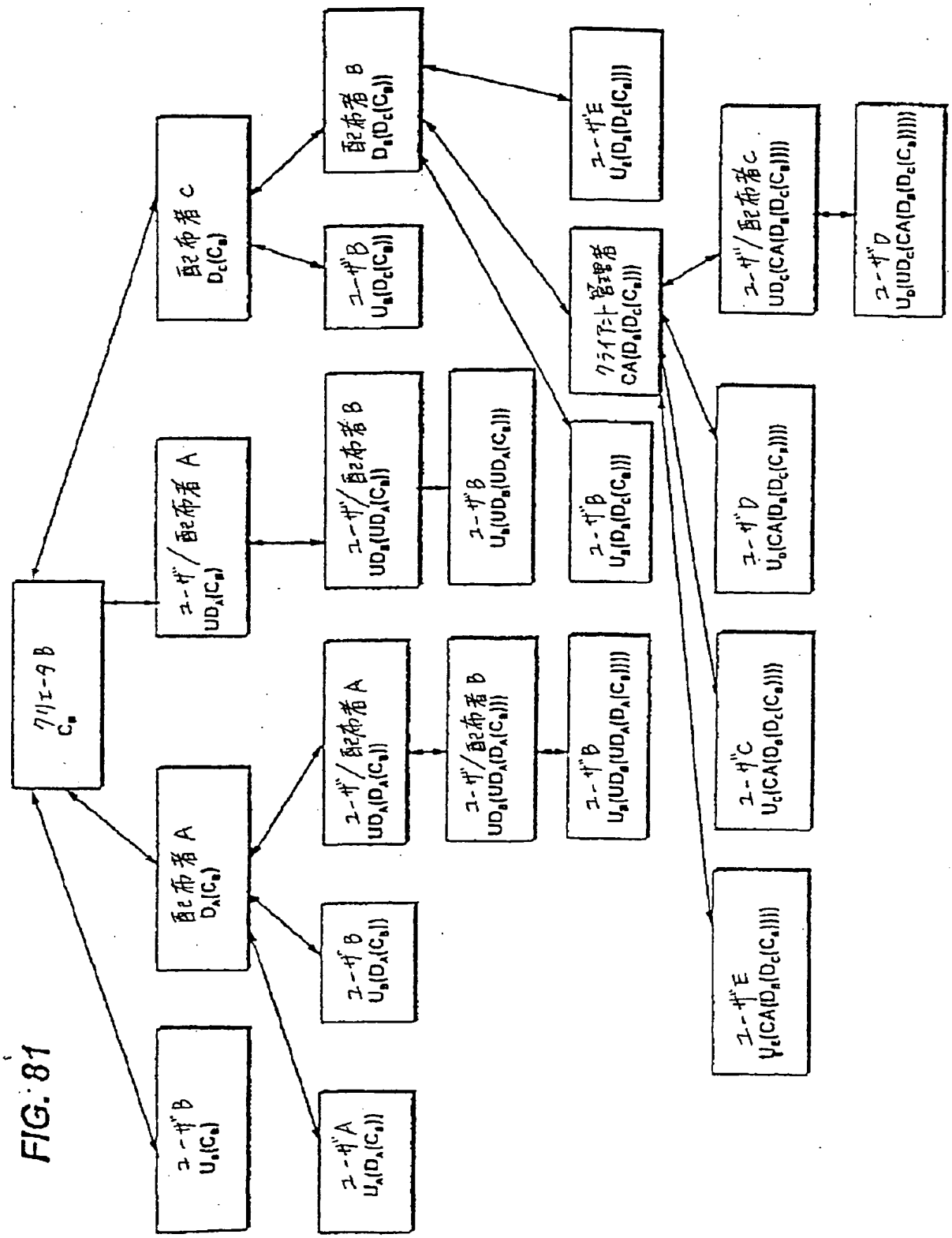

クリエータ B
C_B
配布者 A
D_A(C_B)
配布者 C
D_C(C_B)
ユーザ' A
U_A(D_A(C_B))
ユーザ' B
U_B(D_A(C_B))
ユーザ' B
U_B(D_C(C_B))
ユーザ' A/配布者 A
UD_A(D_A(C_B))
ユーザ' A/配布者 A
UD_A(UD_A(C_B))
ユーザ' B
U_B(UD_A(D_A(C_B)))
ユーザ' B
U_B(UD_A(UD_A(C_B)))
配布者 B
D_B(D_C(C_B))
ユーザ' A/配布者 B
UD_A(UD_B(C_B))
ユーザ' B
U_B(UD_B(UD_A(C_B)))
ユーザ' B
U_B(UD_B(D_C(C_B)))
ユーザ' B
U_B(UD_B(UD_A(D_A(C_B))))
ユーザ' E
U_E(D_B(D_C(C_B)))
クライアント管理者
CA(D_B(D_C(C_B)))
ユーザ' A/配布者 C
UD_C(CA(D_B(D_C(C_B))))
ユーザ' C
U_C(CA(D_B(D_C(C_B))))
ユーザ' D
U_D(CA(D_B(D_C(C_B))))
ユーザ' D
U_D(UD_C(CA(D_B(D_C(C_B)))))
ユーザ' E
U_E(CA(D_B(D_C(C_B))))

FIG. 81

【図82】

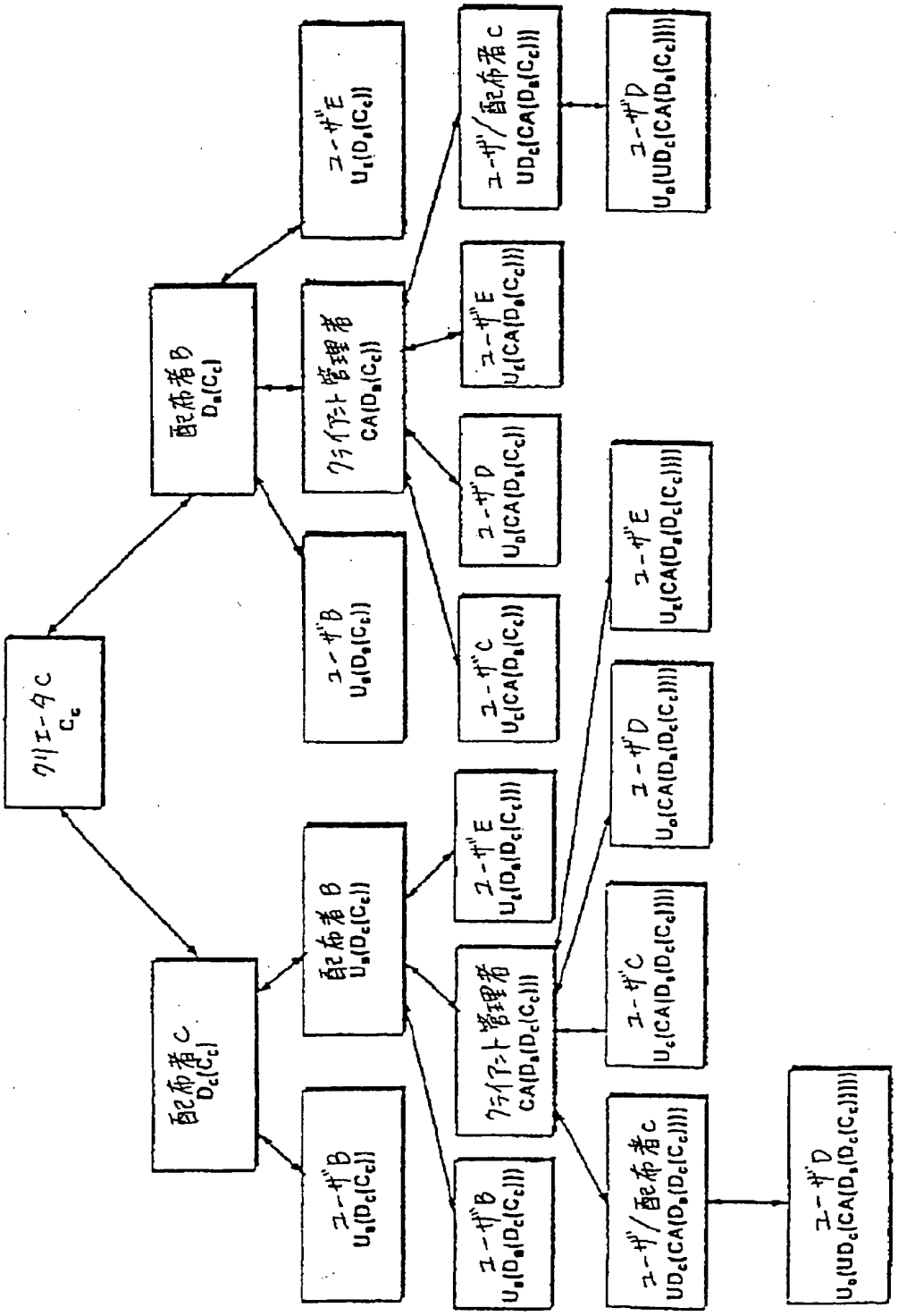
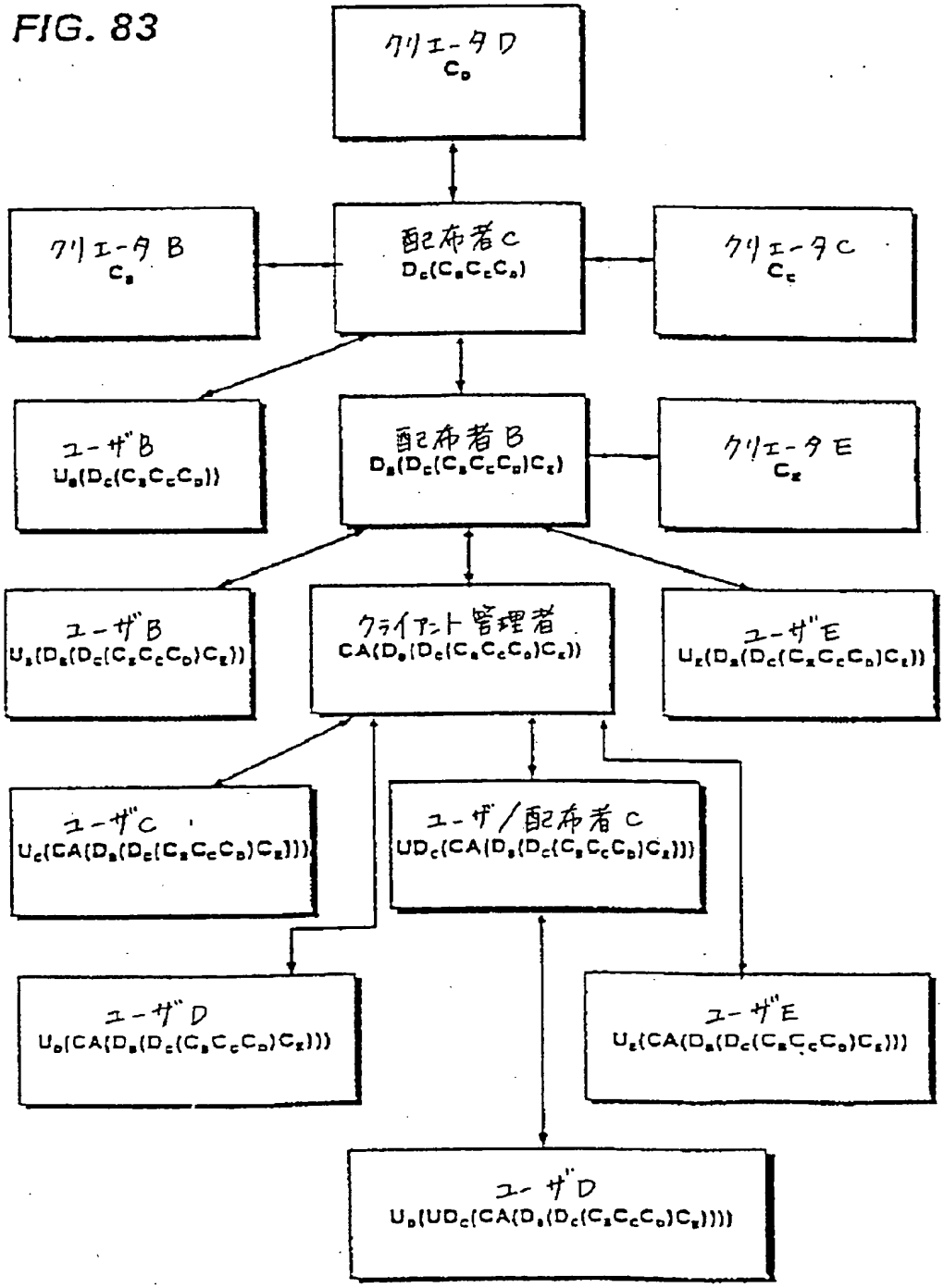

クリエータC
C_c
配布者B
$D_B(C_c)$
ユーザ'E
$U_E(D_B(C_c))$
ユーザ'B
$U_B(D_B(C_c))$
クライアント管理者
$CA(D_B(C_c))$
ユーザ'E
$U_E(CA(D_B(C_c)))$
ユーザ'D
$U_D(CA(D_B(C_c)))$
ユーザ'C
$U_C(CA(D_B(C_c)))$
ユーザ'/配布者C
$UD_C(CA(D_B(C_c)))$
ユーザ'D
$U_D(UD_C(CA(D_B(C_c))))$
配布者C
$D_C(C_c)$
配布者B
$D_B(D_C(C_c))$
ユーザ'B
$U_B(D_C(C_c))$
ユーザ'E
$U_E(D_B(D_C(C_c)))$
クライアント管理者
$CA(D_B(D_C(C_c)))$
ユーザ'B
$U_B(D_B(D_C(C_c)))$
ユーザ'E
$U_E(CA(D_B(D_C(C_c))))$
ユーザ'D
$U_D(CA(D_B(D_C(C_c))))$
ユーザ'C
$U_C(CA(D_B(D_C(C_c))))$
ユーザ'/配布者C
$UD_C(CA(D_B(D_C(C_c))))$
ユーザ'D
$U_D(UD_C(CA(D_B(D_C(C_c)))))$

FIG. 82

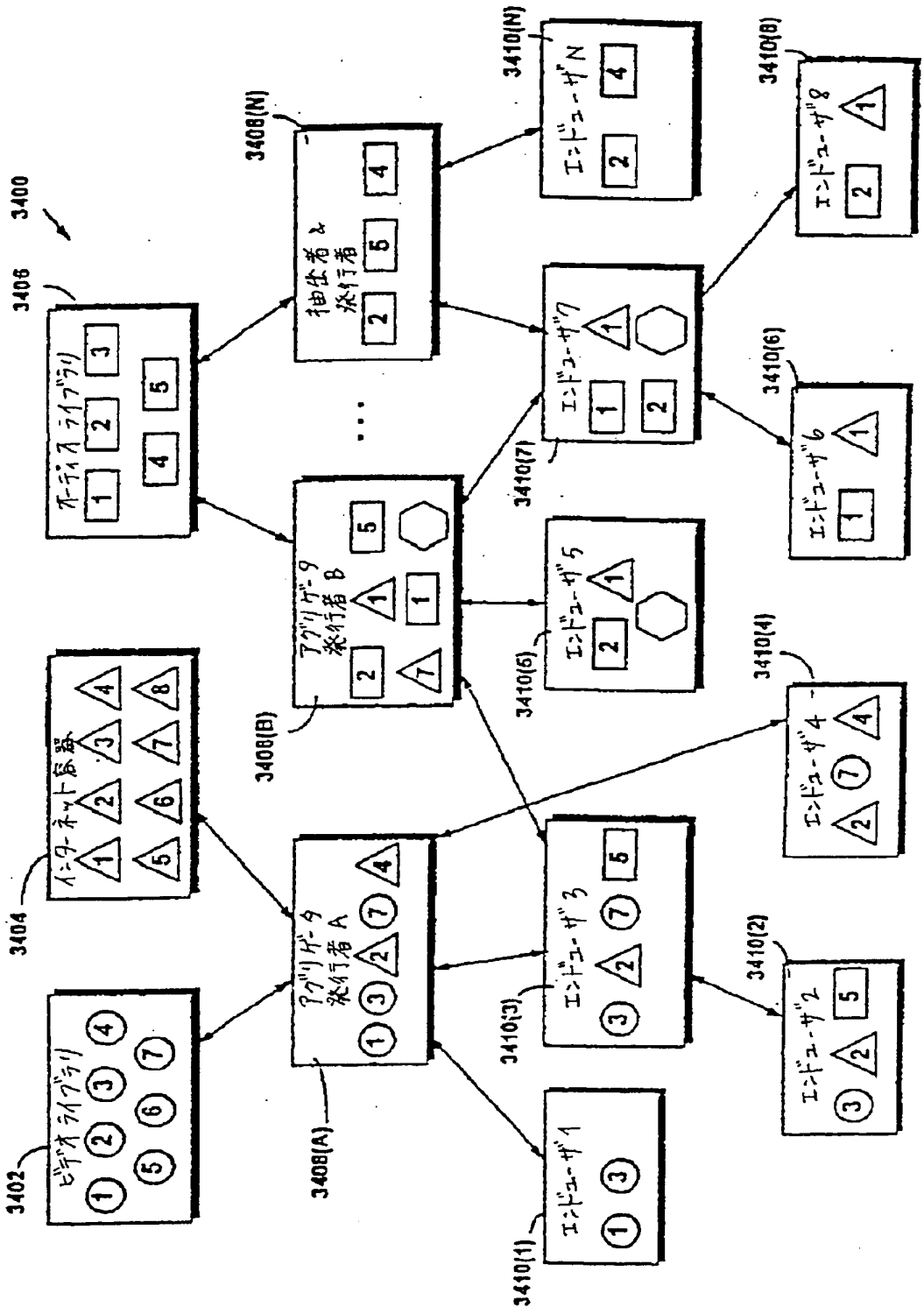
［図８３］

FIG. 83


クリエータD
C_D
クリエータB
C_B
配布者C
$D_C(C_BC_CC_D)$
クリエータC
C_C
ユーザB
$U_B(D_C(C_BC_CC_D))$
配布者B
$D_B(D_C(C_BC_CC_D)C_E)$
クリエータE
C_E
ユーザB
$U_B(D_B(D_C(C_BC_CC_D)C_E))$
クライアント管理者
$CA(D_B(D_C(C_BC_CC_D)C_E))$
ユーザE
$U_E(D_B(D_C(C_BC_CC_D)C_E))$
ユーザC
$U_C(CA(D_B(D_C(C_BC_CC_D)C_E)))$
ユーザ/配布者C
$UD_C(CA(D_B(D_C(C_BC_CC_D)C_E)))$
ユーザD
$U_D(CA(D_B(D_C(C_BC_CC_D)C_E)))$
ユーザE
$U_E(CA(D_B(D_C(C_BC_CC_D)C_E)))$
ユーザD
$U_D(UD_C(CA(D_B(D_C(C_BC_CC_D)C_E))))$

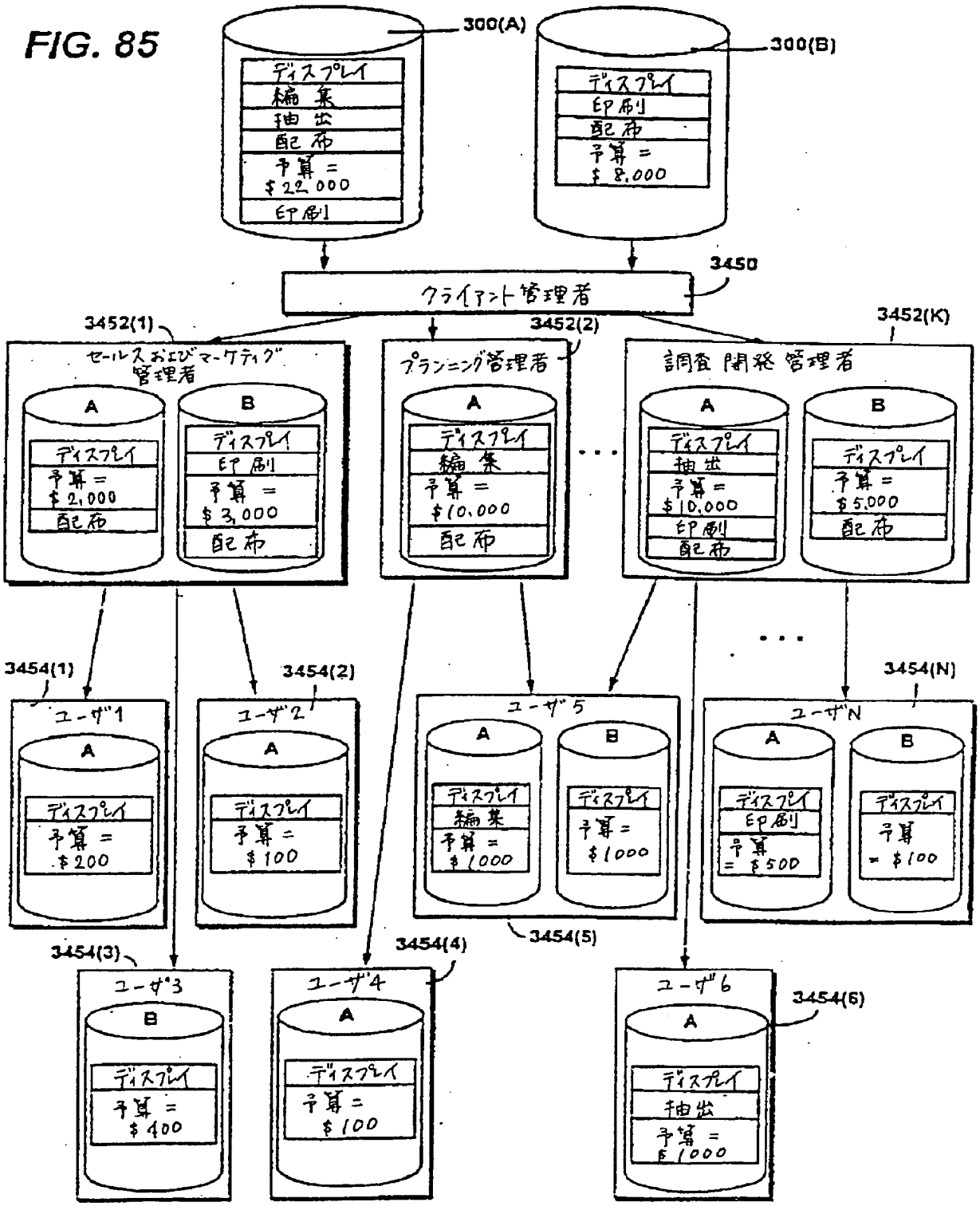
【図84】

FIG. 84

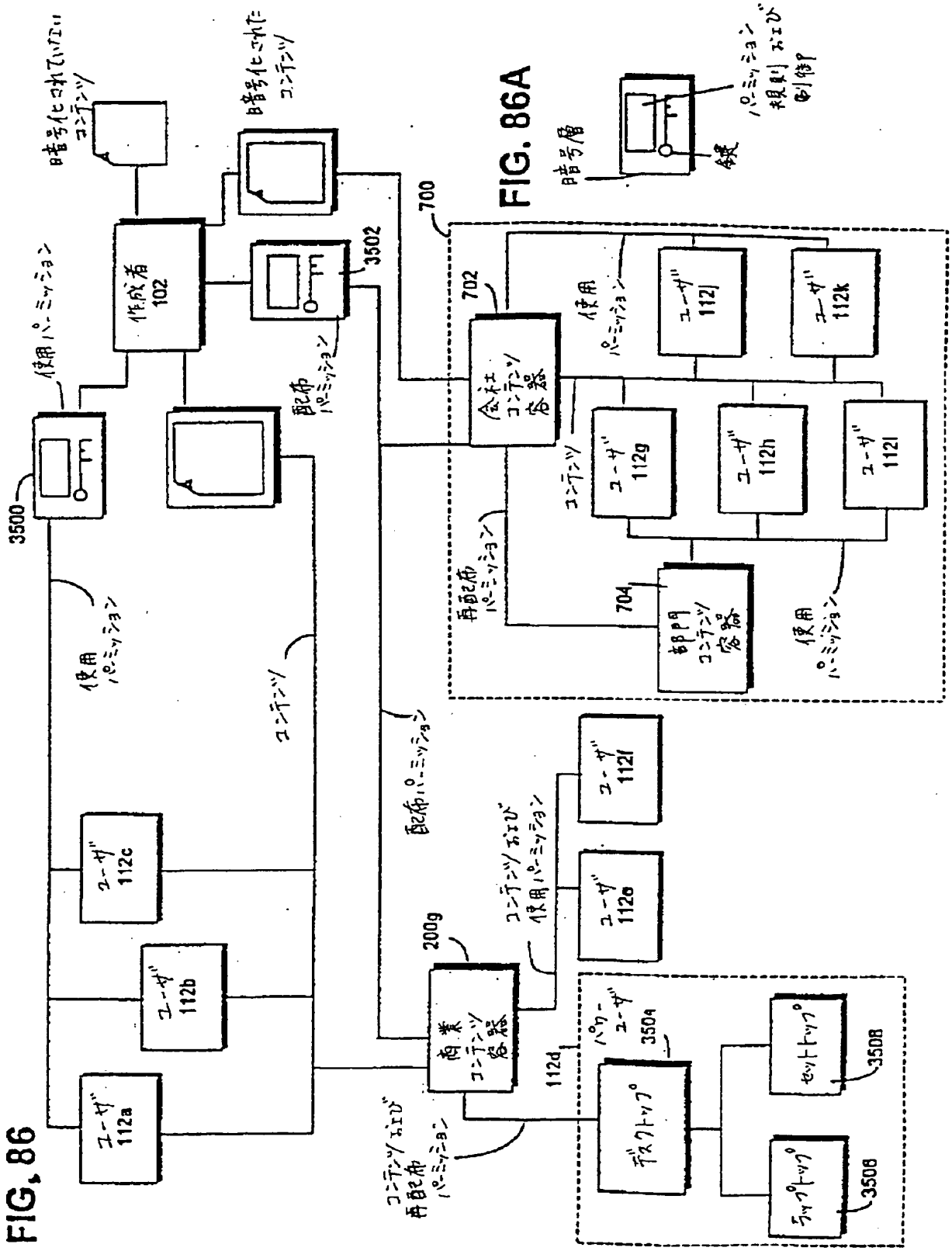

3400
3402
3404
3406
3408(A)
3408(B)
3408(N)
3410(1)
3410(2)
3410(3)
3410(4)
3410(5)
3410(6)
3410(7)
3410(8)
3410(N)
ビデオライブラリ
インターネット装置
オーディオライブラリ
エンドユーザ1
エンドユーザ2
エンドユーザ3
エンドユーザ4
エンドユーザ5
エンドユーザ6
エンドユーザ7
エンドユーザ8
エンドユーザN

【図８５】

FIG. 85


300(A)
ディスプレイ
編集
抽出
配布
予算＝
$22,000
印刷
300(B)
ディスプレイ
印刷
配布
予算＝
$8,000
3450
クライアント管理者
3452(1)
セールスおよびマーケティング
管理者
A
ディスプレイ
予算＝
$2,000
配布
B
ディスプレイ
印刷
予算＝
$3,000
配布
3452(2)
プランニング管理者
A
ディスプレイ
編集
予算＝
$10,000
配布
3452(K)
調査開発管理者
A
ディスプレイ
抽出
予算＝
$10,000
印刷
配布
B
ディスプレイ
予算＝
$5,000
配布
3454(1)
ユーザ1
A
ディスプレイ
予算＝
$200
3454(2)
ユーザ2
A
ディスプレイ
予算＝
$100
3454(3)
ユーザ3
B
ディスプレイ
予算＝
$400
3454(4)
ユーザ4
A
ディスプレイ
予算＝
$100
3454(5)
ユーザ5
A
ディスプレイ
編集
予算＝
$1000
B
ディスプレイ
予算＝
$1000
3454(6)
ユーザ6
A
ディスプレイ
抽出
予算＝
$1000
3454(N)
ユーザN
A
ディスプレイ
印刷
予算
＝$500
B
ディスプレイ
予算
＝$100

【図86】


FIG. 86
FIG. 86A
作成者 102
3500
3502
700
702
704
200g
112d
3504
3508
3508
暗号化されていない コンテンツ
暗号化された コンテンツ
使用 パーミッション
配布 パーミッション
コンテンツ
コンテンツ および 使用パーミッション
コンテンツ および 再配布 パーミッション
再配布 パーミッション
使用 パーミッション
暗号層
鍵
パーミッション 規則 および 制御
全社 コンテンツ 容器
部門 コンテンツ 容器
商業 コンテンツ 容器
ユーザ" 112a
ユーザ" 112b
ユーザ" 112c
ユーザ" 112g
ユーザ" 112h
ユーザ" 112i
ユーザ" 112j
ユーザ" 112k
ユーザ" 112l
パワー ユーザ"
ディスクトップ
ディスクトップ
セットトップ
セットトップ

【図87】

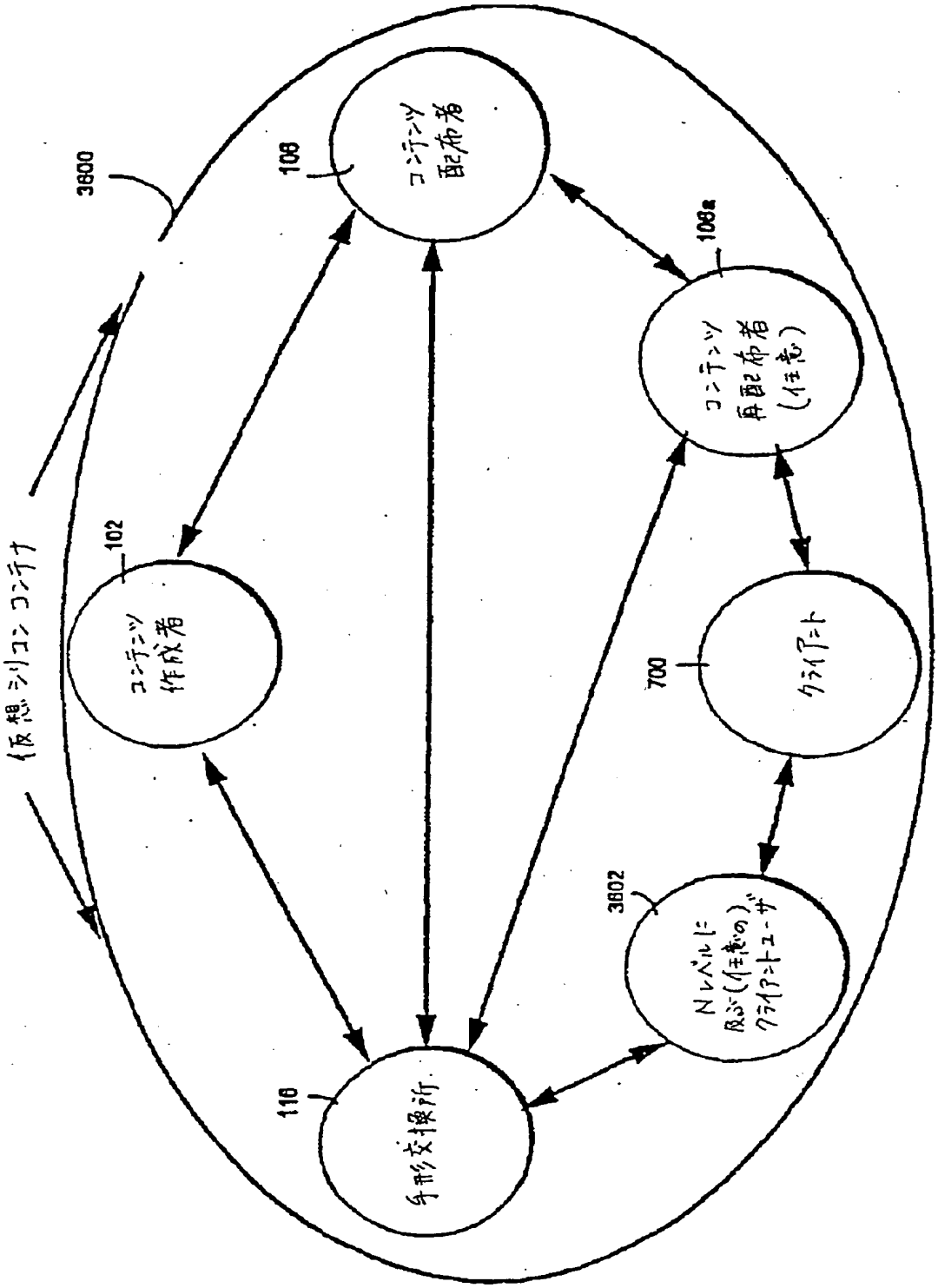

仮想シリコンコンテナ
3600
コンテンツ作成者
102
コンテンツ配布者
108
コンテンツ再配布者（任意）
108a
クライアント
700
Nレベルに及ぶ（任意の）クライアント-サーバ
3602
多形交換所
116

FIG. 87

【国際調査報告】

INTERNATIONAL SEARCH REPORT

Interna' l Application No
PCT/US 96/02303

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6　G06F1/00　　G06F17/60

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6　G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
	-/--	

[X] Further documents are listed in the continuation of box C.　　[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
18 April 1997	14. 05. 97
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Authorized officer Powell, D

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Internat'l Application No
PCT/US 96/02303

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 90 02382 A (INDATA CORP) 8 March 1990 see abstract; figures 2,15 see page 18, last paragraph - page 21, paragraph 2	1,2,5,6, 23,24, 62-65, 68,69, 72-77, 99-102, 133-138, 147-152, 155-158, 199,200
Y	see page 23, last paragraph - page 24, paragraph 1	21,22, 29,30, 103-108, 127-130, 223,224, 233,234, 237,238, 241-244, 504,506
A	--- -/--	61,143, 144,207, 208,245, 246, 487-500, 507-509

INTERNATIONAL SEARCH REPORT

Internal Application No
PCT/US 96/02303

C(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 319 705 A (HALTER BERNARD J ET AL) 7 June 1994 see abstract; figures 2,4,12 see column 4, line 33 - column 6, line 24 see column 24, line 33 - column 25, line 13	7-12, 17-20, 72-77, 133,134, 147-152, 155-158, 265-268, 298,300, 363,396
Y		21,22, 109,110, 115, 203-206, 213,214, 223,224, 237,238, 265, 302-305, 394,395
A		25,26, 31-38, 127-132, 207,208, 370-374, 381-384, 404

-/--

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 96/02303

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	TRANSACTIONS OF THE INSTITUTE OF ELECTRONICS, INFORMATION AND COMMUNICATION ENGINEERS OF JAPAN, vol. E73, no. 7, July 1990, TOKYO, JP, pages 1133-1146, XP000159229 R.MORI ET AL: "Superdistribution: The Concept and the Architecture"	72-77, 99-102, 127-134
Y	see abstract; figure 1 see page 1134, left-hand column, line 25 - page 1135, right-hand column, line 27	29,30, 103-108, 127-130, 233,234, 241-244, 504,506
A		31-38, 153,154, 219,220, 231,232, 370-374, 381-384, 494-497, 501-503, 511,512
X	EP 0 128 672 A (GALE IRA DENNIS) 19 December 1984 see abstract; figure 1 see page 11, line 1 - line 18	78,79, 139-142
A		80,81, 197,525
X	US 4 672 572 A (ALSBERG PETER) 9 June 1987 see abstract; figures 1,2,5,8	83,84
Y	see column 2, line 9 - column 3, line 26	109,110, 115, 302-305, 394,395
A		245,246, 253,254
Y	EP 0 565 314 A (FISCHER ADDISON M) 13 October 1993 see abstract	243,265

-/--

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 96/02303

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 4 799 156 A (SHAVIT EYAL ET AL) 17 January 1989 see abstract; figure 2 see column 7, line 47 - column 8, line 54 see column 9, line 7 - column 11, line 35	42-44, 203-206, 213,214
A		153,154, 207,208, 225-228, 370-374, 381-384, 494-497, 501-503

Y	MAPPING NEW APPLICATIONS ONTO NEW TECHNOLOGIES, ZURICH, MAR. 8 - 10, 1988, no. -, 8 March 1988, PLATTNER B;GUNZBURGER P, pages 45-52, XP000215989 SIUDA K: "SECURITY SERVICES IN TELECOMMUNICATIONS NETWORKS" see the whole document	42-44
A		31-38, 55-58, 95,153, 154,231, 232

Y	EP 0 399 822 A (HEWLETT PACKARD CO) 28 November 1990 see the whole document	87-89

Y	GB 2 264 796 A (IBM) 8 September 1993 see the whole document	87-89

A	WO 92 22870 A (ICL DATA AB) 23 December 1992 see the whole document	93-98, 277-280, 306-318, 342-349, 375-379, 385, 387-393

A	US 5 343 527 A (MOORE JAMES W) 30 August 1994 see the whole document	93-98, 277-280, 306-318, 342-349, 375-379, 385, 387-393

	-/--	

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 96/02383

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 421 409 A (IBM) 10 April 1991 see the whole document	225-228, 245,246, 253,254
A	US 5 103 476 A (WAITE DAVID P ET AL) 7 April 1992 see the whole document	319, 321-340
A	US 5 111 390 A (KETCHAM LARRY R) 5 May 1992 see the whole document	319, 321-340
A	US 4 823 264 A (DEMING GILBERT R) 18 April 1989	
A	IBM TECHNICAL DISCLOSURE BULLETIN, vol. 37, no. 3, 1 March 1994, pages 413-417, XP000441522 "MULTIMEDIA MIXED OBJECT ENVELOPES SUPORTING A GRADUATED FEE SCHEME VIA ENCRYPTION"	
A	US 5 224 163 A (GASSER MORRIE ET AL) 29 June 1993	
A	WO 94 06103 A (HNC INC) 17 March 1994	
A	IBM TECHNICAL DISCLOSURE BULLETIN, vol. 37, no. 48, 1 April 1994, pages 523-525, XP000451335 "TRANSFORMER RULES STRATEGY FOR SOFTWARE DISTRIBUTION MECHANISM-SUPPORT PRODUCTS"	
A	WO 94 03859 A (INT STANDARD ELECTRIC CORP) 17 February 1994	

INTERNATIONAL SEARCH REPORT

Ir　national application No.
PCT/US 96/02303

Box I　Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This International Search Report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the International Application that do not comply with the prescribed requirements to such an extent that no meaningful International Search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II　Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

see annexed sheets.

1. ☐ As all required additional search fees were timely paid by the applicant, this International Search Report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☒ As only some of the required additional search fees were timely paid by the applicant, this International Search Report covers only those claims for which fees were paid, specifically claims Nos.:

Inventions: 3, 6,7,9,10,24 and 29

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this International Search Report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☐ No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT

International Application No. PCT/US 96/02303

FURTHER INFORMATION CONTINUED FROM PCT/ISA/210

The following (groups of) inventions have been identified:

Invention	Claims	Subject matter
1.	1-12,17-26,29,30,61-65,68, 69,72-77,99-108,127-130, 133-138,147-152,155-158, 199,200,219-222,233,234, 243,244,265-268,294-301, 383,364,398,404,504,506	Solving problems related to: Distributing electronic information to a rightful destination using a different virtual distribution environment node (than either supplier or destination) to process the control information associated with the said digital information (cf. either of documents D1 and D2)
2.	13-16	Solving problems related to: Automating electronic processes.
3.	31-39,42-45,55-58,153,154, 203-208,213-218,223-228, 231,232,237,238,241,242, 370-374,381-384,487-489, 500,505,507-512	Solving problems related to: Electronic commerce.
4.	40,41,46-54,259-262,402	Solving problems related to: Identification of principals or principals' properties.
5.	59,60,66,67,70,71,235,236, 239,240,401	Solving problems related to: Handling electronic currency.
6.	78-81,139-144,197,525	Solving problems related to: Tamper-resistant containers.
7.	82-84,109-116,127-132, 273-278,302-305,394,395, 494-497,501-503	Solving problems related to: Audit or administrative information.
8.	85,86	Solving problems related to: Human readable interfaces.
9.	87-92,201,202,209,210,282, 283	Solving problems related to: Event or task processing.
10.	93-98,277-280,306-318, 342-349,375-379,385, 387-393	Solving problems related to: Checking component integrity or validity.
11.	117-122	Solving problems related to: Compromising a security system.

INTERNATIONAL SEARCH REPORT

International Application No. PCT/US 96/ 02303

FURTHER INFORMATION CONTINUED FROM PCT/ISA/210

12.	123-126	Solving problems related to: Electronic data fingerprinting.
13.	159,160,194-196,400,516, 523,524	Solving problems related to: Secure processors.
14.	161-166,517	Solving problems related to: Video controllers.
15.	167-172,175,176,518,519	Solving problems related to: Network communications.
16.	173,174,520	Solving problems related to: CD-ROM controllers.
17.	177,178,521	Solving problems related to: Set-top controllers.
18.	179-185,522	Solving problems related to: Electronic games.
19.	188-193	Solving problems related to: Multimedia communications.
20.	198,526	Solving problems related to: Detection of power supply interruption.
21.	145,146	Solving problems related to: Bitmap data structures.
22.	211,212	Solving problems related to: Modular control structures.
23.	229,230	Solving problems related to: Billing and budgeting.
24.	245,246,253,254,341, 350-353,360-362	Solving problems related to: Protected processing operations.
25.	27,28,247-252,513-515	Solving problems related to: Secure database management.
26.	263,264	Solving problems related to: Secure electronic mail.
27.	269-272	Solving problems related to: Controlling a robot.

INTERNATIONAL SEARCH REPORT

International Application No. PCT/US 96/ 02303

FURTHER INFORMATION CONTINUED FROM PCT/ISA/210

28.	284-293,482-486	Solving problems related to: Business automation.
29.	318,321-340	Solving problems related to: Software construction.
30.	320,359,380	Solving problems related to: Resource management.
31.	354-359,365-368	Solving problems related to: Combining or modifying data.
32.	397	Solving problems related to: Point of sale systems.
33.	398,399,490-493,498,499	Solving problems related to: Advertising.
34.	403	Solving problems related to: Renting an appliance.
35.	255-258,281,386	Solving problems related to: Rights described in software.

A concise analysis shows that the Special Technical Features of these 35 groups of claims, as determined by comparison with the features disclosed in either of documents D1 or D2, are not the same. A comparison of the objective problems related to these different groups of inventions, all seen in the light of the description and the drawings of the application, shows that these objective problems are all different and have no corresponding technical effect.

Consequently, the Special Technical Features of these different groups of inventions are neither the same nor corresponding as defined in Rule 13.2 PCT, 2nd sentence, and therefore the requirement of Unity of Invention (Rule 13.1, 2 PCT) has not been fulfilled.

Finally, it should be noted that searching the additional subject-matter of any of the groups of claims 2-35 would have involved a considerable additional search effort.

INTERNATIONAL SEARCH REPORT

...mation on patent family members

International Application No
PCT/US 96/02303

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9002382 A	08-03-90	AU 4188289 A	23-03-90
		EP 0472521 A	04-03-92
		US 5247575 A	21-09-93
US 5319705 A	07-06-94	JP 7093148 A	07-04-95
EP 0128672 A	19-12-84	WO 8404614 A	22-11-84
US 4672572 A	09-06-87	NONE	
EP 0565314 A	13-10-93	AU 3560793 A	07-10-93
		CA 2093094 A	07-10-93
		JP 6295286 A	21-10-94
		US 5390247 A	14-02-95
		US 5337360 A	09-08-94
US 4799156 A	17-01-89	CA 1281417 A	12-03-91
		EP 0370146 A	30-05-90
EP 0399822 A	28-11-90	US 5075847 A	24-12-91
		JP 3034018 A	14-02-91
GB 2264796 A	08-09-93	EP 0582681 A	16-02-94
		WO 9318454 A	16-09-93
WO 9222870 A	23-12-92	AU 660997 B	13-07-95
		AU 2022792 A	12-01-93
		DE 69203454 D	17-08-95
		EP 0588898 A	30-03-94
		ES 2078051 T	01-12-95
		FI 935541 A	10-02-94
		JP 6509430 T	20-10-94
		SE 9200604 A	13-12-92
		US 5602993 A	11-02-97
US 5343527 A	30-08-94	NONE	
EP 0421409 A	10-04-91	US 5048085 A	10-09-91
		CA 2026739 A,C	07-04-91
		JP 3237551 A	23-10-91

INTERNATIONAL SEARCH REPORT

...rmation on patent family members

Internat... Application No
PCT/US 96/02303

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0421409 A		US 5148481 A	15-09-92
US 5103476 A	07-04-92	CA 2095723 A	08-05-92
		EP 0556305 A	25-08-93
		JP 7089345 B	27-09-95
		JP 6501120 T	27-01-94
		WO 9209160 A	29-05-92
		US 5222134 A	22-06-93
US 5111390 A	05-05-92	NONE	
US 4823264 A	18-04-89	NONE	
US 5224163 A	29-06-93	NONE	
WO 9406103 A	17-03-94	AU 4850093 A	29-03-94
		CA 2144868 A	17-03-94
		EP 0669032 A	30-08-95
		JP 8504284 T	07-05-96
WO 9403859 A	17-02-94	EP 0606401 A	20-07-94
		JP 7502847 T	23-03-95

Form PCT/ISA/210 (patent family annex) (July 1992)

フロントページの続き

(51)Int.Cl.'		識別記号	FI		
G06F	17/60		G09C	1/00	660F
	19/00				660G
G09C	1/00	660	G06F	15/21	330
				15/40	370F
				15/30	L
H04L	9/32				360
			H04L	9/00	671

(81)指定国　EP(AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OA(BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG), AP(KE, LS, MW, SD, SZ, UG), UA(AZ, BY, KG, KZ, RU, TJ, TM), AL, AM, AT, AU, AZ, BB, BG, BR, BY, CA, CH, CN, CZ, DE, DK, EE, ES, FI, GB, GE, HU, IS, JP, KE, KG, KP, KR, KZ, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, TJ, TM, TR, TT, UA, UG, UZ, VN

(72)発明者　スパーン，フランシス　ジェイ．
アメリカ合衆国　カリフォルニア　94530，エル　セリト，エドワーズ　アベニュー　2410
バン　ウィー，デイビッド　エム．
アメリカ合衆国　カリフォルニア　94086，サニーベール，レイクサイド　ドライブ

Best Available Copy